Cloud Security

Attacks, Techniques, Tools, and Challenges

Contents

Preface

We are living in the era of cloud computing, where services are provisioned to the users on demand and 'pay-per-use' basis from a resource pool. Cloud computing has evolved gradually over a period of time. National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, ubiquitous and on-demand network access to a shared pool of computing resources (e.g., servers, network, storage and applications) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Users are gradually adopting cloud services because of the ease and flexibility with cloud services. Most of the companies are changing the way they operate and moving toward cloud-based services.

However, attacking incidents are also increasing day by day with the evolution of cloud computing. Security in such a complex technological environment is very important for providing assurance to cloud customers. Any vulnerability present in cloud, can allow the attacker to gain illegal privileges of Virtual Machine (VM) users. A malicious user can install advanced malware programs and gain higher access privileges (guest OS kernel privilege). A compromised guest kernel can call malicious drivers and can perform malicious actions. Once a VM is fully compromised, an attacker can try to launch attacks such as spreading malwares (virus, worm, etc.), flooding and scanning other VMs. A compromised VM is a big threat to cloud infrastructure which can bypass the security of other VMs. It could further lead to monetary disputes between cloud service provider (CSP) and legitimate VM users. Other than VM Security, there exist various other security issues related to application level, Network level, Virtualization level, Data storage level, Identity management and Role-based access control, Cryptographic key management level, SLA and trust level, Auditing, governance and regulatory compliance and Cloud & CSP migration level security, discussed in the book in detail.

Hence, the importance of well-organized architecture and security roles have become greater with the popularity of cloud computing. People are working in the cloud security domain have proposed various security frameworks to tackle with security threats. The existing frameworks that deploy security tool at individual Tenant Virtual Machine (TVM) are prone to subversion attacks. They are less efficient in detecting malicious activities. Moreover, the TVM-layer security solutions cannot be directly applied at the Virtual Machine Monitor (VMM)-layer because of the semantic gap problem at the hypervisor. Semantic gap refers to interpreting the low-level information of a

guest OS into a high-level semantics. VM introspection (VMI) is one of the virtualization-specific approaches that provides possible ways to obtain the high-level view of TVM at hypervisor.

However, not enough work has been done in this direction to provide VMI-based security solutions for cloud. The existing VMM-layer solutions do not provide a complete solution to detect both basic and evasive malware attacks in cloud. On the other hand, some of the cloud security frameworks are designed to detect network intrusions only. Most of them apply signature-matching technique as core detection technique, making them prone to signature-manipulation attacks. This book provides an in depth understanding various security techniques with their short comings. It also talks about various advances in cloud security.

In this book, we have endeavored to provide a technical foundation that will be practically useful not just for professional cloud security analysts conducting security practices but also for students, independent researchers, and all those who are curious in the field of cloud security.

Audience:

This book is intended for both academic and professional audiences. As a textbook, it is intended as a semester course at under graduate and post graduate level students in Computer Science, Information Technology, Network Security, and Information Science and Management. The book serves as basic reference volume for researchers in cloud security. It will be useful to practitioners, cloud security team, and the cloud security auditor as well. To get the most out of this book, the reader should have a working knowledge of various operating system environments, hypervisors, cloud computing fundamentals, programming languages like Python and Java, and a working knowledge of security tools.

Organization of the book:

The book is organized to provide a broad overview of the important topics of Cloud security. It is divided into three parts: "Fundamentals," "Threat model, attacks & defensive techniques," and "Tools & Advances."

Part I, "Fundamentals," covers the basic concept of cloud computing and Cloud Security. This provides a foundation for more advanced topics, which are covered in the next two parts. Part I includes the following chapters:
Chapter 1: "Introduction to Cloud Computing" presents an introduction to key domain considered and gives the brief background history of Cloud Computing. The chapter also discusses the characteristics, service models and deployment models and associated open research challenges.
Chapter 2: "Introduction to Cloud Security" presents various vulnerabilities along with cloud security concepts, standards and cloud security reference architectures.

Chapter 3: "Cloud Security and Privacy Issues" presents various cloud security goals and concepts, security issues, requirements for privacy and security.

Part II, "Threat model, attacks, defensive systems and security techniques," discusses threats and attacks along with major mechanisms which can be applied to cloud security.

Chapter 4: "Threat model and Cloud Attacks" covers the threat model and various possible attacks at various layers in Cloud Computing.
Chapter 5: "Classification of various IDS in Cloud" covers the types and characteristics of various Cloud-IDS and provides future research directions.
Chapter 6: "Intrusion Detection Techniques in Cloud" discusses various misuse, anomaly, virtual machine introspection and hypervisor introspection techniques used to protect the cloud from attacks.

Part III, "Tools and Advances," covers various tools and advance topics such as introspection and container security.

Chapter 7: "Overview of Tools in Cloud" covers the classification of various attacking and security tools and case study of LibVMI, a hypervisor-based security tool.
Chapter 8: "Virtual Machine Introspection and Hypervisor Introspection" covers the advanced virtualization specific cloud security techniques used to protect the virtual domain and hypervisor in Cloud.
Chapter 9: "Container Security" covers the threat model and attacks in containerized environment. It also discusses various defensive mechanisms and open challenges. A case study on the Sql Injection attack in Docker systems is also demonstrated.

Tools:

This book is designed to be accessible to a wide audience to teach the fundamental principles and techniques of cloud security. There are many tools available to perform various attacking activities, taking memory snapshots both from inside the VM and outside the VM and analyzing and extracted log files. The focus is to provide the technical insight by providing the detailed classification of attacking and security tools along with case studies of some attacking and security tools.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Acknowledgment

This book is a result of our research work at the Malaviya National Institute of Technology Jaipur, Graphic Era University Dehradun and Doon University Dehradun. The book has been inspired by our research works published in reputed journals in the area of Cloud Security. I would like to offer special thanks to co-authors Prof. Vijay Varadharajan (Global Innovative Chair in Cybersecurtiy, The University of Newcastle Callaghan, Australia) and Dr. Udaya Tupakula (Senior Lecturer, The University of Newcastle Callaghan, Australia) for their excellent guidance. We have thoroughly updated our work and included state-of-the-art practices, reference architectures, standards, security and attack tools, and case studies in Cloud Security. We have included advanced topics such as Virtual Machine Introspection, Hypervisor Introspection, and Container Security.

We would like to thank Prof. Surekha Dangwal, Vice Chancellor Doon University Dehradun, Prof. Udaykumar R. Yaragatti, Director MNIT Jaipur and Prof. Kamal Ghanshala, President Graphic Era Deemed to be University Dehradun who have wholeheartedly supported the writing of this book.

We gratefully recognize the opportunity Taylor and Francis gave us to write this book. We like to make a special mention of thanks to all the splendid staff specially Shikha Garg (Senior Editorial Assistant, CRC Press—Taylor & Francis Group), Aastha Sharma (Senior Acquisitions Editor, CRC Press—Taylor & Francis Group), Isha Singh (Editorial Assistant, CRC Press- Taylor & Francis Group), and Shashi Kumar (Senior Assistant Manager, KnowledgeWorks Global Ltd) who put so much time and effort into producing this book. They were ever ready to incorporate many editing changes made by us during the proof reading phase.

Dr. Mishra would like to thank her entire family as the journey would never have been possible without their support. She specially thanks her mother Mrs. Sarla Mishra and father Mr. Diwakar Mishra for always supporting her in all possible ways in all difficult and good times. She also thanks her husband Mr. Deepak Joshi for his support and motivation, daughter Divyanshi Joshi for keeping her active and happy during this period. She also thanks her father-in-law Mr. P. C. Joshi and mother-in-law Mrs. Kamla Joshi, for always motivating her to do something good. She thanks her brother Mohit and sister-in-law Pinky, for having their joyful company during the final editing phase of this book. Special thanks to her friends Mini Kandpal, Reeta Uniyal, Asha,

Amita, Jharna, Nisha, Sonal, Ritu, Gaurav Varshney, and Ankit Vidyarthi for giving a wonderful company and helping her to overcome stress.

She would like to specially thank the research scholars Umang Garg, Divya Kapil and under graduate students Saurabh Gupta and Phalugni, Saloni for their help during the work and for being the part of her research team. She thanks to the other research team members as well specially under graduate students Palak, Ishita, Kashish, Akansh, Sachin, Shivam, Garima, Rahul Bisht, Rahul Sharma and post graduate students Aparna and Diksha and research scholars Sarishma, Charu Negi for being the part of her security group, named CyberZine.

She would also like to thank her foreign research collaborators specially Dr. Nour Moustafa (Senior Lecturer in Cyber Security and Computing at the School of Engineering and Information Technology (SEIT), University of New South Wales (UNSW)'s UNSW Canberra, Australia) and Dr. Zakirul Alam Bhuiyan (Assistant Professor, Department of Computer and Information Sciences, Director Dependable and Secure System Research (DependSys), Fordham University USA) who are working in the field of security and privacy and have always inspired her to work hard.

Dr. Emmanuel Pilli would like to thank his wife Phoebe Vanmathy Julius and their daughter Pramiti Evangeline.

Prof. Joshi would like to thank all his family members, especially his wife Smt. Usha Joshi and daughters Ira and Bakul.

List of Figures

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

List of Tables

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Author Bios

Preeti Mishra is currently working as Assistant Professor in the Department of Computer Science, Doon University, Dehradun, India. Earlier, she was associated with Graphic Era Deemed to be University Dehradun. She has 10+ years teaching and research experience. She has been awarded Ph.D. in Computer Science and Engineering from Malaviya National Institute of Technology Jaipur, India, under the supervision of Dr. Emmanuel S. Pilli and Prof. Vijay Varadharajan (2017). She is a B. Tech and M. Tech Gold Medalist. She has published various SCI/SCIE indexed reputed international journals and reputed conference papers in the area of security and privacy. Some of her key research publications have been published in IEEE Transaction on Cloud Computing (with IF 5.720), IEEE Communication Surveys and Tutorials (with IF 23.7), IEEE Transactions on Industrial Informatics (IF: 9+), etc. as main author. She has also published several publications in reputed international conferences. She worked as a visiting scholar in Macquarie University Sydeny under Prof. Vijay Varadharajan in 2015 and has been awarded a fellowship, administered by the Department Administrators in Department of Computing, Macquarie University, Sydney. She has also been awarded by Graphic Era Deemed to be University Dehradun for outstanding contribution in research. Her research proposal valued more than 20 lakhs got approved by SERB-DST, Govt. of India in the area of Cloud Security. Her area of interest includes Cloud Security, E-mail Security and Network Security, Internet of Things, Blockchain, Cyber Security, Mobile Security, Adversarial Machine Learning, etc. She is an active reviewer of many reputed international journals/conferences such as *IEEE Transaction on Network and Service Management, Future Generation Computer Systems, IEEE Journal of Information Security and Applications*, etc. She is currently serving as Lead Guest Editor in IEEE Transaction on Industrial Informatics (TII).

Emmanuel S. Pilli received his Ph.D. from IIT, Roorkee (2012) and is currently Associate Professor, Dept. of CSE in Malaviya National Institute of Technology, Jaipur, India. Pilli Emmanuel Shubhakar has 21 years of teaching, research, and administrative experience. He completed a research project "Investigating the Source of Spoofed E- mails" from UCOST, Dehradun in 2016. He has coauthored a book "Fundamentals of Network Forensics—A Research Perspective" for Springer in 2016. A total of four students have been awarded Ph.D. under his supervision and 12 Ph.D students are pursuing their research. He is Senior Member of both IEEE and ACM. His areas of interest

include Security and Forensics, Cloud Computing, Big Data, IoT, Darkweb, and Blockchain, etc. He is member of Cloud Computing Innovation Council of India (CCICI) and Forensic Science Workgroup on Cloud Computing of the NIST, USA.

Dr. R.C. Joshi, former Prof. E. and C.E. Department at IIT Roorkee and Chancellor at Graphic Era University Dehradun, received his B.E. degree from NIT Allahabad in 1967, M.E. 1st Div. with Honors and Ph.D from Roorkee University, now IIT Roorkee, in 1970 and 1980, respectively. He worked as Lecturer in J.K. Institute, Allahabad University during 1967–1968. He joined Roorkee University in 1970 as Lecturer, became Reader in 1980 and Prof. in 1987. He had been Head of Electronics & Computer Engineering from Jan. 1991–1994 and Jan. 1997 to Dec. 1999. He was also the Head of Institute Computer Centre, IIT Roorkee from March 1994 to Dec. 2005. He was on short visiting Professor's Assignment in University of Cincinnati, USA. University of Minnesota, UA and Macquarie University Sydney Australia also visited France under Indo-France collaboration program during June 78 to Nov. 79. Dr. Joshi has guided 27 Ph.Ds, 250 M.Tech, Dissertation, 75 B.E. Projects. He had taught more than 25 subjects in Computer Engineering, Electronics Engineering and Information Technology. He has worked as Principal Investigator in a number of Sponsored Projects of Ministry of Information & Communication Technology, DRDO, AICTE, UNDP, ISEA, etc

Part I

Fundamentals: Cloud Computing and Security

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 1

Overview of Cloud Computing

1.1 Introduction

The era of cloud is the latest trend which provides various types of on-demand services to the user on the basis of 'pay-per-use' manner, depending upon the requirements of the end-users. The cloud computing has gained lots of popularity and gradually it is expanding its services to address millions of user's demand. The vision of cloud computing industries for the 21st century is to grant computing services in a convenient way just like any other basic services like water or electricity [1]. There is no longer a need to invest on IT infrastructure or developing buildings for initial set-up, and hiring skilled workforce, to run a business. Cloud computing allows small business owners to start the business quickly by using cloud services, without thinking about purchasing and setting-ups large infrastructure. Cloud computing uses various technologies such as virtualization, distributed computing, cluster computing, and service-oriented architecture (SOA), etc. [2]. Cloud computing is developing and constantly improving technology that still does not have any unanimous definition. Various opportunities are provided by the cloud computing to the IT industries by offering a variety of services.

The traditional IT enterprise set-up requires a large infrastructure such as big land space, hardware devices, expensive software licenses, and a big team of IT experts for the establishment of the company. As time passes, there is a requirement to upgrade the whole system of hardware and software to maintain the growth and scalability of the company. Hence, it requires lots of money, resources, and time to maintain and provision the services in traditional way. It makes traditional computing less economical way to start a new business or upgrade the existing ones. Therefore, cloud offers a better economical solution to address the need of organizations. In cloud computing, there is no need to care about the failure and maintenance of any hardware and software services. Developers can focus more on their coding skills rather than focusing on setting up the test environment by downloading and installing various software [3].

Cloud computing is one of the evolving technologies which has been widely used for IT outsourcing, infrastructure provisioning, platform provisioning, software provisioning and database provisioning, etc. Let us now define the

DOI: 10.1201/9781003004486-1

cloud computing term in a more formal way. Cloud is a term that has been used historically by the telecommunication industries as an abstraction of the network for the representation of the system diagram. Cloud computing refers to an Internet-centric computing with virtual infrastructure. The National Institute of Standard and Technology (NIST) proposed a definition of cloud computing [4]. As per this definition "Cloud computing is a 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". The definition is more focused on three main characteristics: (i) Cloud services are scalable, (ii) The overall cost is charged on the basis of usage, and (iii) The quality of services is distributed and managed to the clients.

Foster et al. [5] described grid computing along the concept of cloud computing. Authors described the cloud computing as a kind of distributed computing that is focused on the large-scale paradigm that contains a abstracted pool, scalable, virtualized, dynamic, managed computation resources, large storage and virtual platforms, which are delivered on-demand through the Internet. The adoption of cloud services such as deployment environment, infrastructure, or applications has different impact on the industries. There are several perspectives which can have the potential benefits of cloud services such as: (i) It provides a simple process to establish an environment for application development, (ii) It provides the potential to shorten the process of idea to product, (iii) It provides better solution for the business community, (iv) Simplifies the process for application development, and (v) Provides assurance of the quality of services like security and availability when required [6]. However, there are still many issues which need to be addressed by the vendors before provisioning any of the services online.

Let us now understand the technical terminologies of cloud architecture. An OpenStack [7] cloud architecture is considered here a base model. OpenStack is a global leading cloud management software opted by many companies for developing cloud platform for public, private, or hybrid cloud. It will be discussed in forthcoming sections. The key technology in the cloud environment is virtualization which creates an abstraction layer above the underlying hardware or software. It hides the complexity of physical hardware and allows multiple operating systems to run on the same physical machine. The abstraction layer is called as Virtual Machine Monitor (VMM) or Hypervisor. The cloud architecture with Xen as VMM is considered here. Xen VMM is booted first as a primary boot system. Afterward, Linux kernel is loaded as Dom0 domain by the Hypervisor. Dom0 is the privileged domain (administrative VM) which is used to control, configure, and manage all the other VMs by the cloud administrator. Dom0 runs the device drivers and can access the actual hardware, as shown in Figure 1.1. The networking between the TVMs is provided by VMM. Networking in VMM bridges the virtual adapter to the physical adapter. The tenant virtual machines (TVMs) are loaded after

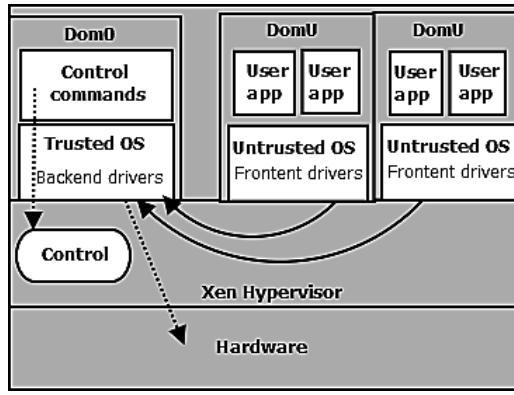

FIGURE 1.1: Basic architecture of Xen.

Dom0 and are also referred as untrusted domains (DomUs). VMM has the highest privilege and full control over any VM running over it. Let us now start understanding the cloud computing architecture.

A cloud environment typically consists of three types of servers: Cloud Controller Server (CCS), Cloud Compute Server (CCoS), and Cloud Networking Server (CNS) [8], as shown in Figure 1.2. The CCS is mainly used to handle all management-related work. The user VMs are hosted in CCoS server. The CNS manages the network, routes the packets, and allocates IPs to the nodes, etc. There are three types of cloud network: administrative, ex-

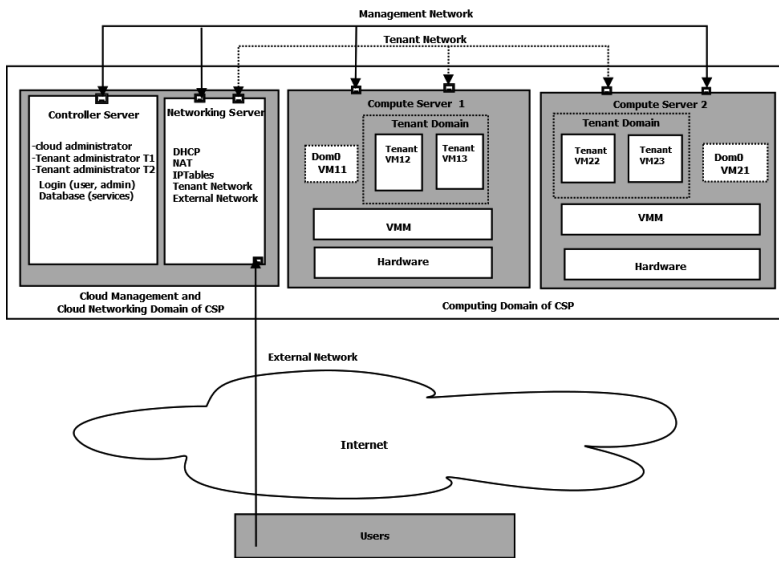

FIGURE 1.2: Basic architecture of cloud environment.

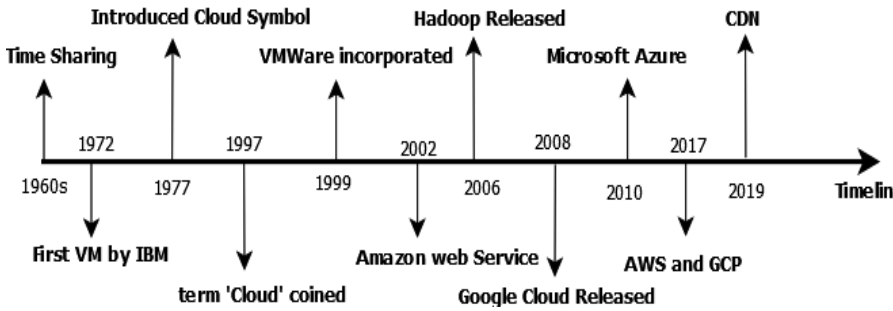

FIGURE 1.3: History of cloud computing.

ternal, and tenant network. The tenant network carries the tenant's data and ensures the end-to-end transportation. Each tenant network connects a set of VMs and is vulnerable to the threats. The administrative network mainly deals with carrying the data corresponding to management commands such as allocating, destroying, creating, and resuming TVM. The external network connects cloud VMs to the external users via Internet. The administrator of the cloud can configure the entire access control policies and has got highest privileges in cloud environment.

1.2 History and Underlying Technologies

Basically, cloud computing is not a new idea or a new technology. It has been evolved over the years. A brief history of cloud computing is shown in the Figure 1.3. In the 1960s, John McCarthy [9] already anticipated that there will be some computing facilities available for the general public like a utility. In the same year, IBM and DEC used to provide their computers on sharing basis [10]. IBM announced its first VM which runs on the physical hardware, and creates the virtual machine environment in the year 1972 [11]. The cloud symbol was used in the year 1977 [12]. In the 1990s, the term cloud has been used to describe a large ATM network. After the evolution of Internet and world wide web, the term 'cloud' is coined by Ramesh Chellapa in the year 1997 [13]. In the year 2006, it was used to describe a business model by Google's CEO Eric Schmidt [14]. After that, it gained a lot of popularity. Since then, cloud computing has been mainly used to represent as a marketing term in several business ideas. In July 2008, some big giants like HP, Yahoo, and Intel announced a global computing laboratory, cloud computing, which enriched with a variety of platforms for sharing the resources and technology in the area of cloud [14]. Voas and Zhang [15] demonstrated six different

phases of cloud computing evolution. Firstly, end-users can interact with a mainframe which supports multiple applications. Users can interact directly with their own system which drops the hardware cost with high computational power. Resource sharing can be done through a type of network either LAN or WAN in the third phase. The Internet services can provide access to remote services with an active account pay-per-basis. The next phase provides high-performance computing and throughput using grid computing. Finally, it provides all computing services through the Internet.

The concept of cloud computing is an outcome of evolution and advancements of many other technologies, which makes cloud computing more powerful. As the technologies grow, it introduces several emergences with other key technologies. However, there are some key technologies that played a key role in the development of cloud computing like mainframe, grid computing, web 2.0, or service-oriented computing, etc. Let us now discuss some of the key technologies:

1.2.1 Mainframe computing

Mainframe [16] is one of the key technologies which has large computational facilities with multiple processing units. It provides large input-output operations, reliable computational technology, massive data movements, and powerful tools. Generally, this kind of technology is used by large industries for the transfer of bulk data, online transactions, resource planning, and operations that are dealing with large input-output operations. Mainframes offer a large computational platform with multiple processors that has the ability to process the data as a single entity. Mainframes have a great feature of sustaining computationally expensive load for many hours. It can handle all kinds of failures transparently. The systems were highly reliable due to the replacement of the faulty components without shutting down the system. The key feature of the mainframe systems was batch processing. Although the popularity of these systems is reduced nowadays. Some latest versions of the system are still used in online transactions, airline ticketing, and several government online platforms, etc.

1.2.2 Cluster computing

Cluster computing [17] is an alternative or a low-cost choice to the supercomputers or mainframes. Cluster computing is a set of connected computers with a high bandwidth network that behaves as a single unit. It can be controlled by some set of tools. (as shown in Figure 1.4). These computers are connected through a local area network and run its own instance of an operating system. Cluster computing provides high-speed computing and parallel computing in the 1980s [1]. The main advantage of these systems is that they have very cheap cost as compared with the mainframe computers and used in some small organizations. Cluster computing has emerged with a several

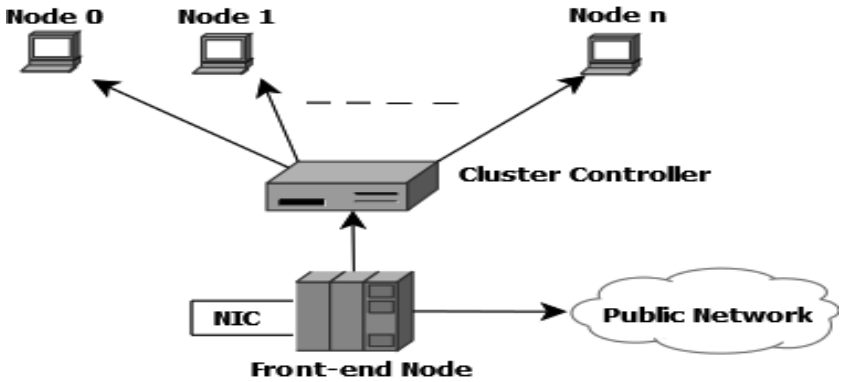

FIGURE 1.4: Cluster computing.

high-speed processors, low-cost platforms with connectivity, and software tools for distributed computing. These kinds of systems provide higher reliability due to easy detection and replacement of a faulty node. Load-balancing and high-availability clusters improve the overall performance. The evolution of cluster computing has contributed a lot toward the development of parallel virtual machine (PVM) and message passing interface (MPI). It also provides the ability to provide scalability if required with the increasing demand of computational power.

1.2.3 Grid computing

In the early 1990s, grid computing [18] was introduced as an evolution of cluster computing. It also makes use of group of physically connected computers to execute a single dedicated operation and to solve some complex problems. A grid is connected using a grid middleware software which is used to translate the information from one format to another recognizable format. Let us differentiate between the cluster and grid computing. Grid computing nodes can be dispersed geographically and heterogeneous; whereas in cluster computing, all nodes must be managed in a single location with a network. Grid computing is also known as the predecessor of cloud computing due to its processing power and distributed nature. The architecture of grid computing can be used for redundant network connection and load-balancing environment. The major benefit of grid computing is that it provides parallel processing which enables a developer to divide a program into small segments and solve the same each segment problem independently and then combine the results of each segment to produce a single solution. Grid computing can be used for a large organization where several machines are sitting idle at a particular moment.

1.2.4 Distributed and parallel computing

In the early 21st century, there were requirements of multiprocessor design and faster programs to solve complex problems. Distributed and parallel computing [19] address the problem and act as a foundational model of cloud computing that supports connectivity of multiple nodes with a network. The parallel and distributed computing provides several basic services like consistency in memory updation, concurrency, mutual exclusion, message-passing, and shared-memory. The major difference between these two is that distributed computing supports multiple processors that may be distributed in different nodes and connected via memory channel using a common network. Whereas parallel computing supports multiple processors deployed in same node and communicate with shared memory bus. There are two kinds of processor architecture in parallel computing: tightly coupled and loosely coupled architectures. Tightly coupled multiprocessors are able to share memory and communicate by information exchange among processors. In loosely coupled multiprocessors, communication can be done by sending messages to each other across the physical links. The most efficient topology of parallel computing is a hypercube, in which each node is connected directly with some neighbors.

1.2.5 Virtualization

Virtualization [20] is introduced around 40 years ago but it has limited number of applications. It has not been utilized efficiently due to resource constraints. However, these limitations have overcome and it has become the foundational element of cloud. Virtualization allows the end-user to access several computation technologies and storing components on-demand with a pay-per-use basis. The main utilization of virtualization is that it simulates the interface between hardware and end-user. Virtualization can be integrated with several latest technologies, which helps in developing a powerful computing environment. Hardware virtualization integrated with the software stack provides the platform called virtual machine instances. Several virtual machine instances can be executed on high performance computers. To replicate the runtime environment of programs, virtualization can be used. There are several types of virtualization types such as hardware, software, storage, and operating system virtualization. Virtualization is supported by specialized software such as Hypervisor which provides connectivity between the server and the virtual environment.

1.2.6 Web 2.0

A web interface is required through which cloud computing can deliver its services. Currently, the web has been evolved with several services and functionalities like interactive sharing, collaboration, the composition of application,

and user-centered design. Web 2.0 [21] is the current state of online technology that provides several new features as compared to the web. It provides the better user interaction, improved channels, and collaboration. Web 2.0 is an extended and dynamic version of the web which is able to share information online through social media, Internet, and web-based communities. There are several advantages of web 2.0 such as rich web application, latest technical specification, user-friendly, and dynamic learning communities. There are several applications of web 2.0 such as Google Maps, Flicker, Facebook, Blogger, and YouTube. Flicker provides some advanced services to store digital images, videos, and online diaries. It brings interactivity and flexibility of the web pages to improve the user experience using web-based access for desktop applications. Finally, the main aim of web 2.0 is to leverage the utility of the Internet to everyone.

1.2.7 Service-oriented computing (SOC)

SOC [22] is the foundational model for cloud computing and provides support to the low-cost, flexible, and interoperable system. A good SOC model must have the following properties like loosely coupled, platform-independent, and transparent to the location. It is difficult to endeavor to adopt the SOC due to the early stage of the technology and incompleteness of web services. There are several standards for web services such as Web Services Description Language (WSDL), the Simple Object Access Protocol (SOAP), and the Business Process Execution Language (BPEL). SOC introduced two main concepts such as Software-as-a-service (SaaS) and quality of service. The term SaaS has been inherited from the application service provider (ASP) that delivers the software services across the world on-demand and rental basis. Quality of service requirements can be shared among the client and the providers. SOC relies on service-oriented architecture (SOA) to build a service model and a way to recognize applications and infrastructure. SOA is capable of the service discovery, integration, and overcome different challenges of distributed computing.

1.2.8 Utility computing

It provides computational services through an on-demand and pay-per-use basis. Utility computing [23] is a popular IT service that provides flexibility to the end-user. Users can access these services economically. Utility computing is a model that is very similar to basic service models such as electricity, telephone, and gas. The end-user can access the services virtually using a virtual private network through the Internet. The back-end services and infrastructure is managed by the service providers. There are several applications of utility computing such as grid computing, cloud computing, and managed IT services. It also includes some basic storage functionalities like virtual storage, virtual server backup, virtual software platform, online backup, and most IT

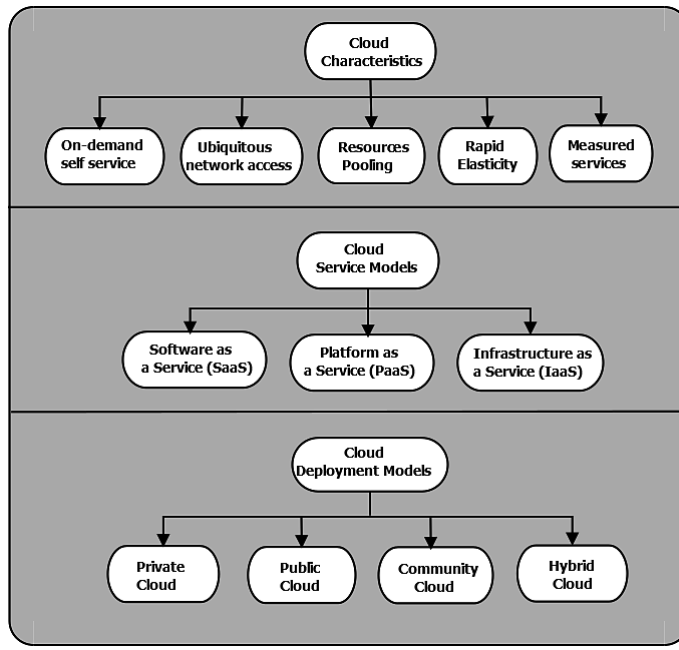

FIGURE 1.5: Cloud characteristics, service models, and deployment models.

solutions. Scalability, elasticity, virtualization, automation, and standard utility computing are some of the characteristics of utility computing. The main advantage of this model is that it reduces the cost of IT services, hardware, and optimum utilization of existing services.

Let us understand the cloud characteristics, deployment models, and service models which are explained in below sections and also shown in Figure 1.5.

1.3 Definitions and Characteristics

The US Department of Commerce introduced an agency that is responsible for providing standards in the field of Science and Technology, named the National Institute of Standards and Technology (NIST). The NIST worked continuously and after the 15th version. The NIST definition [24] of cloud computing presents, "Cloud computing is a 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." According to the NIST, few characteristics of cloud are as [4]: broad network access, on-demand self-service, rapid elasticity, resource pooling, or expansion, and measured service.

- **On Demand Self Service:** Email, services of server, application, or network kind of computer services can be provided without explicit intervention of the service provider. It also ensures that the customer can perform all the required actions himself without any help from IT experts. For example – any request of the consumer must be automatically processed by the cloud platform, without explicit interaction of the provider.
- **Broad Network Access:** The NIST ensures that the services of cloud computing are available over the network through the Internet, which can be used by diverse consumers like IoT devices, cell phones, and laptops.
- **Resource Pooling:** To serve the multiple consumers with different geographical locations, providers used to pool the virtual resources and dynamically assign them to the clients on-demand. At the higher level of abstraction, customers must be able to specify locations like country, data-center, etc.
- **Rapid Elasticity:** To scale on-demand, the capabilities available can be elastically provisioned and released. The rapid elasticity can be disbursed to provide the quantity.
- **Measured Services:** Cloud service can automatically control and optimize resources at the level of abstraction according to the service type. The resources should be monitored, controlled, and reported to have transparency for all customers as well as provider.

1.4 Cloud Service Models

The cloud computing model is capable of providing convenient, on-demand, and ubiquitous network access to storage, and services that can be provisioned with minimal intervention. The cloud service providers (CSPs) ensure that the cloud services are having the computational capabilities which can support the essential characteristics of cloud computing. There is three kinds of possible service models provided by cloud computing such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [25]. The major factors to categorized cloud services are the cloud service customers (CSCs) like end-user, IT operations, or developers, and computing

capabilities like software, infrastructure, or platform. As per the NIST cloud computing reference architecture (CCRA), the services are available at the service layer of the orchestration layer. The explanations of the services are as follows.

1.4.1 Software-as-a-service (SaaS)

SaaS [26] model enables the access to cloud-based web application with the existing infrastructure of the organizations. The SaaS applications run on the CSP's side and maintained and controlled by the vendors. The services can be accessed with a paid licensed subscription, or for free but with limited access. To access the services of the cloud, one is not supposed to install any new application, infrastructure, or software. The major benefits of SaaS are affordability, ready-to-use, affordable, and accessible anywhere. There is no requirement of having on-premise hardware for the cloud service model which is opted by small-scale organizations. These services can be accessed anywhere with Internet connectivity. The applications integrated with the SaaS are ready to use services and require no set-up or installation. Although there are several benefits of this service model, some demerits are also there in the SaaS model like lack of control (full access of the vendors) and slower speed (applications are accessed through the Internet and run in remote servers). The SaaS-based cloud services have fewer features and functionalities as compared to the client-server co-relations. Although these disadvantages can be avoid if the organization deals with the offered features only.

1.4.2 Platform-as-a-service (PaaS)

A third-party vendor provides a platform through which we can develop, test, or run the applications. PaaS [27] service model has the capability to eliminate the need for in-house premises hardware and software installations. Unlike SaaS, we can control and manage the underlying cloud platform through the deployed applications. Default services are offered in terms of the servers, networking, or storage manageable by the vendors or the platform providers. The main advantages of the Paas service model are cost-effectiveness, multiple programming language support, scalability, minimum development time, and enhanced collaboration. In the PaaS model, it is difficult to switch from one PaaS vendor to another vendor, which is the major drawback of this model. PaaS model is having some security and compatibility issues with the cloud model. So, due to compatibility issues, we may be required to leave some elements out of the cloud model.

1.4.3 Infrastructure-as-a-service (IaaS)

IaaS [28] is the most flexible cloud model which provides the complete and scalable control over the customization and management with existing

infrastructure. This model has the capability to replace the traditional infrastructure components and on-premise data-centers like servers, networking devices, and storage units. It provides a virtual provision of computing services over the cloud through the Internet. Amazon Web Services, Microsoft Azure, and Google engines are some of the examples of the CSPs. Minimized capital cost, simple deployment, and flexibility are the main advantages of the IaaS model. In the IaaS model, it is very easy to deploy the servers, storage, and networking for smooth functioning. However, the cost of the IaaS model is more than the PaaS or SaaS model. It's difficult to get the detailed insight details of the IaaS model due to restrictions imposed by cloud admin.

1.5 Cloud Deployment Models

Cloud services are the future of IT solutions which is all about outsourcing the services and infrastructure to access it through the Internet. The growth of cloud computing enhances the service deployment models [29] and its strategies. So, there are several enterprises of cloud solutions which depend on the degree of required outsourcing. To enable the fast-loading, there are thousands of servers and storage devices of cloud hubs. Cloud hubs are given the priorities to the user according to the closeness of the user's geographical location. Therefore, the deployment models of cloud computing can be categorized based on geographical location. A more specific categorization is provided according to the administrative domains of the cloud. The categories of various deployment models are as follows.

1.5.1 Private cloud

Private cloud [30] can be used by stand-alone organizations. It also provides control over security and backed up by a firewall that can be hosted externally or internally. These kind of clouds are implemented within the campus or a building for private use and generally can be accessible to the organization itself. Private clouds are the best solution for the organizations which require high-security and availability. It also has the possibility of testing applications and systems with low cost as compared to other cloud services. Some key advantages of private clouds are as follows:

- **Information Protection:** The first and major key advantage of private cloud is to keep the information safe within the premises of the organization. Although several public cloud vendors claim for the good quality services with high-security. There are lots of vulnerabilities which are founded by several hackers in the past.

- **Assure Service Level Agreements:** Data replication, monitoring and maintenance, recovery, and appropriate recovery mechanisms are some of the requirements which are expected from the private cloud to ensure the quality of services. Although public cloud vendors provide some of the features. All features can be achieved through the private cloud.
- **Compliance Using Procedure:** To deploy and execute some applications through any third-party services, the standard procedure and operations need to be ensured. It may not be possible for virtual public infrastructure.

These kinds of services and benefits make the private cloud more secure and available for better services. If we consider the architectural view, private clouds are heterogeneous in nature due to deployment using existing infrastructure. It could be a desktop grid, a cluster, a data-center, or a combination of them. Although private cloud has lots of features, they have limited capability to scale elastically on-demand when compared with the public clouds.

1.5.2 Public cloud

Public cloud [31] services are provided for public use through a network for general use. End-users do not have any control over the location of infrastructure. The canonical viewpoint of the public clouds says that services are available with anyone, from anywhere using the Internet. Public clouds are available as a shared cost model or pay-per-use per user basis. These kinds of model are best suited for the growing or variable requirement organizations. They offer the solution to minimize the IT infrastructure cost and can handle the existing infrastructure. There are some key advantages of public clouds.

- **Multi-tenancy:** A public cloud has a multitude of users, not as a single user and a user can work in a virtual environment separately than the other users. This is one of the primary requirements to provide effective monitoring of the user and provide quality of services.
- **Ubiquitous Model:** A public cloud is able to offer all three service models such as platform (for example, Google AppEngine), infrastructure (for example, Amazon EC2), and Software (for example, salesforce.com).
- **Less Restrictions:** If we consider an architectural view of public clouds, there are very few restrictions. Public clouds can be composed of geographically dispersed data-centers to share the load of users and to serve server them according to their locations.

These kinds of clouds are having several benefits but less secure due to availability for the general users. Public clouds also provide a wide range of services to the end-user with the existing infrastructure. So, there is no need to set-up high configuration hardware or software to start a new organization.

1.5.3 Community cloud

Community clouds [32] are distributed systems that can be created with the help of distinguishing cloud integration to address the specific requirements. Basically, it is a mutually shared model among several organizations which are belonging to a particular community like government agencies, banks, scientific research, and commercial organizations, etc. These models of cloud can be developed by an internal employees or third-party vendors by multiple administrative domains. Some key benefits of community clouds are discussed as below:

- **Control and Convenience:** Community clouds have enough flexibility to design it as per the requirements. So, there is no conflict between control and convenience that can make all decisions through a collective effort.
- **Environmental Sustainability:** Community clouds are supposed to emit less carbon due to the under-utilization of resources. So, these clouds tend to provide more environmental sustainability.
- **No Single Point of Failure:** There are multiple administrative hosts that provide infrastructure and support to the community cloud. If there is one system failure, then the remaining system will work properly.

A community cloud can also be formed as an aggregation of the resources of several communities. Community clouds are heterogeneous in nature and independent from the vendor's agreements. These clouds are also known as open systems due to that fair competition among different solutions.

1.5.4 Hybrid cloud

Hybrid cloud [32] consists of a large hardware and software infrastructure that can fulfill the requirements of multiple users. This model combines the best practices of a public and private cloud but as separate entities. A hybrid cloud can provide scalability, security, and flexibility to the end-user. There is an ideal situation of the organization in which an organization uses a private cloud within the organization and uses the public cloud to interact with its customers. There are some key points about hybrid clouds:

- **Scalability:** Hybrid clouds can address the scalability issues and can provide distinguished clouds for different services. For example, to deal within the premises and outside of the premises.
- **Cloud-Bursting:** In the hybrid cloud, we can have several services or resources for a time period till required which can be released after usage. This kind of flexibility is provided by the hybrid cloud and is known as cloud-bursting.

- **Infrastructure Management:** Hybrid clouds provide the facility of infrastructure management software like OpenNebula which is a kind of scheduler that provides cost-based scheduling.

The provisioning of services can leverage the distinguished other services to ensure the quality of services. There are several other benefits of hybrid cloud such as higher efficiency, faster deployment, low upfront cost, and simple to manage infrastructure.

1.6 Cloud Service Platforms

In this section, various cloud service platforms are explained which are offered by various cloud vendors.

1.6.1 Amazon web service (AWS)

Amazon Web Services began its IT infrastructure services for various firms which are provisioning web services. These services are known as cloud computing nowadays. The main advantage of this kind of services is that they replace capital expenditure to operational expenditure (low-cost paradigm). AWS provides a scalable, reliable, and low-cost infrastructure in the cloud that provides hundreds of businesses around the world. AWS provides computation services and various other services to help grow an organization. The services are based on several protocols such as HTTP, REST, and SOAP protocols.

1.6.2 Microsoft azure

Microsoft Azure [33] service is provided for Windows platform that mainly have three components that provide particular services to the end-users such as windows Azure, SQL, dot NET, and azure services. The services run on the cloud servers. For example, the SQL server is offered as a service by SQL azure. The local applications are running through the .net services. There are distinguish services which are offered for the cloud users like virtual machines, identity, storage, mobile services, data management, and messaging, etc.

1.6.3 Google cloud platform

Google provides a cloud platform which is named as Google Compute Engine (GCE) [34]. GCE is the IaaS component that is used for global infrastructure which runs different services such as Gmail, YouTube, Google search engine, and other services. A GCE instance can start with a disk resource that is known as persistent disk. GCE provides the facility to the end users to launch

the virtual machine on demand that can be customized according to their requirements. It provides several features like VM performance, transparent maintenance, billing, pricing model, and global scope for images and snapshots. Google VMs can boot within 30 seconds that is about 4–10 times faster than other VMs.

1.6.4 IBM cloud

IBM provides cloud services [35] which is a public platform with different products like storage, computation, networking, development, testing, security, etc. The operation and management of these services is done by IBM. The IBM cloud platform combines IaaS and PaaS and integrates the services of infrastructure with different platforms. This cloud platform supports both large and small organizations. IBM cloud services are built to support the requirements of public cloud or multi-cloud model. It provides different open-source technologies such as Kubernetes, computation options, Red Hat Openshift, VMs, or containers. Cloud native applications can be deployed to ensure workload portability.

1.6.5 Adobe creative cloud

The video editing, designing of the graphics, web development, and many more services are the collection of software services which are provided by the adobe creative cloud. Adobe creative cloud [36] is available on monthly or annual subscription and delivered via Internet. It retains several features of adobe creative suits with new features like instant upgradation, easy-sharing, storage to the cloud, etc. There are some services provided by the adobe creative cloud such as spark, premier rush, XD, Fonts, and portfolio. It is a tool which enables both collaboration and creativity. It builds fully functional websites from ground data to mobile designing. Creative cloud supports both MAC OS and windows version of the system.

1.6.6 Kamatera

Kamatera [37] is a part of global cloud service provider which contains a rich set of services for all kind of organizations. It uses most advanced technologies with high level of customer services. Kamatera is operating thirteen global data-centers and serving thousands of customers including application developers, international enterprises, SaaS providers, etc. It provides a rich set of services such as cloud server with web hosting, wordpress server hosting, storage, cloud private network, virtual private servers, and many more. Kamatera clients can customize the services of the company according to their requirements and scale their services on hourly or monthly basis.

1.6.7 VMware

VMware [38] is a virtual-machine platform which is an abstraction of x86 PC hardware to execute the multiple operating system in an unmodified way. It indicates that multiple deployments are possible for desktop applications without rebooting or partitioning. VMware cloud comprised SaaS and IaaS which is ideal solution for application service providers (ASPs), Internet service providers (ISPs), and PaaS. The multi-cloud solutions can deliver a cloud operating model for all kind of applications. It is a world's leading public cloud which provides protection and scaling for vSphere-based applications. VMware reduces the overall operational overhead expenses and achieves faster cloud strategy in terms to leveraging the existing skills. It is still continuing to invest on people, innovation, employee productivity, and business.

1.6.8 Rackspace

Rackspace [39] offers cloud backup and block storage. Cloud block storage is released in the year 2012 and powered by OpenStack service. The Rackspace cloud provides cloud-based products and services, which offers cloud storage, virtual private server, load balancer, backup, monitoring, and databases. Rackspace cloud services deliver the innovative capabilities which increase efficiency, and generate new revenue streams. It provides distinguish services such as management of hosting, professional services, security and compliance, business intelligence, and application managed services. It is used to deliver high performance by using solid-state drives and hard drives. Whereas backup services provide file-level backups and compression techniques to improve security.

1.7 Challenges Ahead

Although cloud computing has gained lots of popularity these days due to its adaptability by the industries during a short time period. However, the research in the cloud is still in its initial stage. There are a significant amount of issues that are still needed to be addressed. Several new challenges also keep emerging for industrial growth. In the current section, we discuss some key research challenges of cloud computing.

1.7.1 Virtual machine migration

To balance the load of the data-centers in the cloud computing, virtual machine migration comes into picture. It also enables the CSP to provide the highly responsive and robust mechanism in the data-centers. This process has

been evolved from the process migration techniques, which are used to implement the migration in real-time. Authors of VMware [40] have performed some live migration of VMs which can be implemented in a part of the milliseconds. Another team of authors [41] is able to migrate the entire OS and its applications as a single unit which is able to avoid several problems like migration at the process level and VM level. The main advantage of VM migration is to avoid the hotspot in the real-time, which helps to detect workload hotspot. The secure VM migration is an evolving research area in which research is still going on.

1.7.2 Interoperability and standards

Cloud computing is a kind of service-based model to provide infrastructure such as water and electricity. For the proper utilization of the services, several vendors want to provide interoperability and standards between distinguish solutions. But, vendor lock-in is one of the major obstacles against the growth of cloud services. If an organization wants to switch its CSP, then it requires a considerable amount of time, conversion cost, and resources. Hence, the presence of interoperability and standards provide a room to choose the vendor and switch them easily. There are some organizations that are leading the path to standardize the services of cloud computing such as Cloud Computing Interoperability Forum (CCIF), DMTF Cloud Standards Incubator, and Open Cloud Consortium [42]. Another approach to provide the standards to the cloud is a general reference architecture and a standard interface through which a user can interact.

1.7.3 Security and privacy

A secure communication among cloud nodes [43] helps in meeting the confidentiality and privacy of user's data. To achieve the high-end security among the data-centers, good security measures should be in place. One cannot rely on CSP for providing better security solutions. The providers must achieve the following objectives such as auditability as a check point and confidentiality to secure access. Confidentiality factor can be implemented through the use of encryption techniques, whereas the auditability can be ensured by using remote attestation techniques. These techniques need a trusted platform module as a proof of security. However, remote attestation techniques are not sufficient. Hence, there is a need to build a trust mechanism at each layer of the cloud. The development and deployment of efficient and robust Intrusion Detection System (IDS) is another security challenge in cloud. Specially, some of the intrusions may target hypervisor layer to compromise the entire system. Introspection-based approaches play a vital role to provide cloud-specific security solutions. However, not much research work has been done in this area.

1.7.4 Energy management

There is another issue with the cloud services called as management of energy. The 53% of the total expenditures of the data-centers have invested in powering and cooling of the system [44]. Hence, CSPs have more pressure to reduce this cost and improve the energy efficiency for the operational centers and cut down the total cost. It attracts the researchers to improve the energy-efficient techniques and meet the requirement of government standards as well. There are several solutions to reduce the power consumption provided by several researchers [45] like the architecture based on the energy, scheduling of jobs for energy-aware, and the protocols used for the networking purpose. Although several techniques have been proposed by authors. However, it is more challenging to achieve a trade-off among the application performance and energy-efficient mechanisms.

1.7.5 Accessibility issues

The access control applies to the read and write allowances for [46] authenticated users. The username and password are used to provide the authentication of the system. In the multi-tenant cloud environment, there are a large number of customers. A significant number of customers are in the multi-tenant cloud world. Each client uses website or front-end GUI to access cloud services. Therefore, distinguished and efficient access control techniques are required to be developed to solve the authorization issues.

1.8 Conclusion

Cloud computing has gained popularity in recent time to manage and deliver services through the Internet. Cloud computing can provision applications, storage space, and several software services as per the demand of users. The ultimate aim of cloud computing is to deliver the services as pay-per-go manner just like basic services such as water and electricity. In fact, a small industry or start-ups can initiate their work without any pre-defined hardware or software requirements. However, despite of having significant advantages provided by cloud computing, there are several key challenges which are still not covered by researchers like energy management, security, trust, interoperability, etc. We also provided some few definitions with the discussion on history of cloud computing. Various key technologies have also been surveyed with the emergence of cloud. The standard definition with cloud characteristics has also been covered in the current chapter. Various cloud service models, such as IaaS, PaaS, or SaaS have also been discussed along with cloud deployment models such as private cloud, public cloud, community cloud, and

hybrid cloud. At the end, several research challenges are discussed which provides future research directions.

1.9 Questions

Fill in the blanks

1. Arrange the development of following in ascending order:

i Microsoft Azure
ii Hadoop
iii Google cloud
iv Amazon web services

Mark the correct option for answering the question 1.
(a) iv, iii, ii, i (b) iii, iv, ii, i
(c) ii, iii, iv, i (d) i, ii, iii, iv

2. Which of the following is incorrect statement:

i Applications of web 2.0 are Google map, Flicker and Facebook.
ii A service-oriented computing model must be tightly coupled and platform dependent.
iii Virtualization can be integrated with several latest technologies.
iv Utility computing is used in grid computing and cloud computing.

Mark the correct option for answering question 2.
(a) i (b) iii
(c) ii (d) iv

3. Cloud Computing is used for

i Infrastructure provisioning
ii Platform provisioning
iii Database provisioning

Mark the correct option for answering question 3.
(a) i is true (b) i & ii are true
(c) i, ii & iii (d) none of the above

4. A cloud environment consists of

i Cloud Controller Server
ii Cloud Compute Server

iii Cloud Network Server
iv All above mentioned

5. Cloud bursting is common in

i Hybrid Cloud
ii Private Cloud
iii Public Cloud
iv All above mentioned

Short-Answer Questions

1. Define cloud computing and describe various characteristics of cloud computing.
2. Explain various service delivery models of cloud computing with examples.
3. Discuss various cloud computing deployment models with example scenarios where they are most suitable for.

Long-Answer Questions

1. What is the need of cloud computing. Discuss all the architectural components of cloud architecture with suitable diagram in detail.
2. Discuss how cloud computing is different than traditional computing environment. Explain various open research challenges in cloud.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 2

Introduction to Cloud Security

2.1 Introduction

Cloud security consists of set of technologies, controls and policies designed to protect the applications, infrastructure and data of cloud environment. It can also be considered a sub-branch of computer security and network security. It consists of the security constraints designed to incorporate the cloud service provider and end-user perspectives. The importance of cloud security has been immensely increased in the modern computing era. There are several users who are gradually adopting cloud for hosting their applications and data. However, there are still various concerns which prohibit the users/enterprises/organizations to adopt the cloud-based infrastructure. Cloud Security Alliance (CSA) did a survey in the year 2019 and found that security is the major concern for majority of users [47].

CSA's report stated that a total of 81% users have the security concern while adopting the public cloud platforms. Whereas 62% users are worried about data loss and leakage risks and 57% people are worried about the regulatory compliance as shown in Figure 2.1 [47]. They found 49% users have concern for issues related to integration with rest of non-cloud IT environment while adopting the public cloud infrastructure. Around 44% users have legal and cost related concerns. A total of 39% users are worried about the visibility issues and 35% emphasize more on application-migration related cloud adoption concern. There were 32% users who have concern related to lack of expertise staff to handle the cloud services. There also stated that 23% users have concern of not having a staff to manage cloud services. Only 2% cases were reported for having vendor lock-in related issues.

The flexibility and easiness of cloud services have opened doors for attackers. The attacking incidents which are happening in the cloud-based IT environment, raises a big question for securing cloud environment. Some of the security agencies have reported various attacks such as Virtual Machine Escape, discovered by research outfit VUPEN security [48] in 2012. This attack affected the error handling function of Intel processors. According to the report of European Network and Information Security Agency (ENISA) [49], Dropbox has been affected by Distributed Denial of Service (DDoS) attack. The DDoS botnet was also launched against amazon web services. Hackers

DOI: 10.1201/9781003004486-2

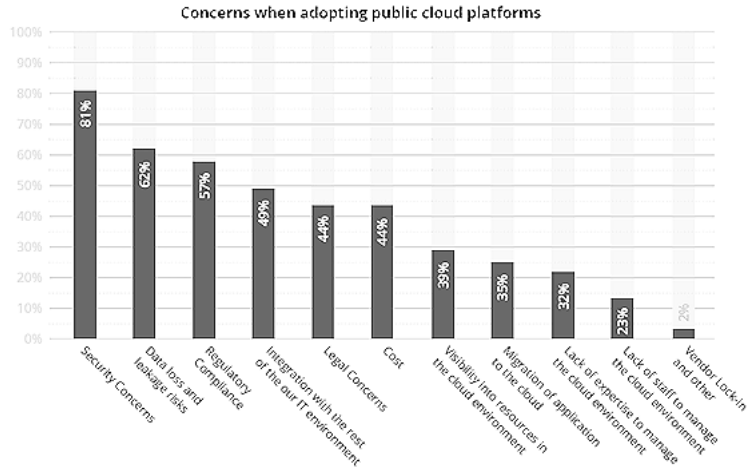

FIGURE 2.1: Concerns shown by enterprizes/user while adopting public cloud infrastructure.

used the exploit in ElasticSearch and attacked the amazon EC2 instances in 2014 [50]. It has also been reported by cyber threat defense that 75% attacks apply the known vulnerabilities which are still present in software in 2014 [51]. Infact Code Space is attacked by attackers, causing destruction of the customer's sensitive data in 2014 [52]. Symantec reported that 494 vulnerabilities and two zero-day vulnerability in 2015 [53].

Internet Security Threat Report stated the proportion of evasive-malware samples in cloud environment that can detect the virtualization environment as shown in Figure 2.2 [54]. Cisco does the recent survey and classified Trojan as top five malware attacks to gain access to user's computer and organization network [55] in 2017. It is one of such attack which gains access to user's computers and network. The investigation carried out by cisco reveals that 75% organizations are victim of malicious software which can be used to launch advanced attacks. As per CSA report in 2018, there were a total of 23420 phishing website links were found which have very high compared to 2016 report [56]. Recently, a cloud service provider company "iNSYNQ" became a victim of ransomeware attack which caused shut down of their network system, making it difficult for customer to access the services on 2019 [57].

The increasing attacking incidence each year raises a concern for security in cloud environment. Below, some of the key vulnerabilities in cloud are discussed which are usually exploited by attackers as shown in Table 2.1.

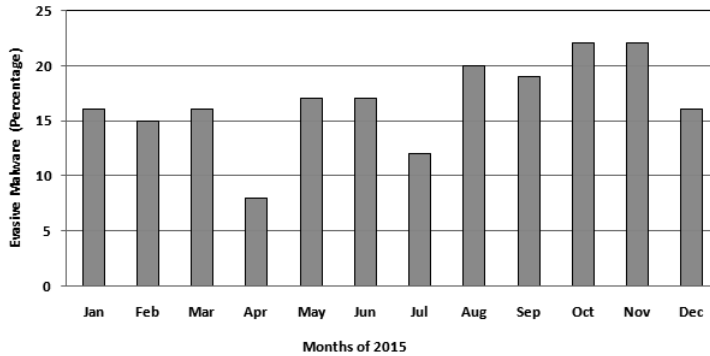

FIGURE 2.2: The attack statistics of virtualization-aware evasive malware samples in cloud environment.

TABLE 2.1: Key vulnerabilities in cloud environment

Vulnerabilities	Consequences
Lack of physical control	Loss of physical control on the data located in remote cloud servers can lead to data leakage and modifications, etc.
Under-provisioning of bandwidth	The under-provisioning of bandwidth can lead to consumption of resources by causing flooding attacks such as DDoS.
Pricing model of cloud	Compromising the billing model of cloud can incur in generating the incorrect billing information, causing disputes between CSP and tenants.
Insecure Browser and APIs	Breaching the securing control through insecure APIs can cause unauthorized access to resources
Illegitimate access to management interface	Attackers can gain the control on the management console and gain access to administrative access.

2.1.1 Vulnerabilities present in cloud

Let us now understand various major vulnerabilities in Cloud Computing.

Vul1 – VM Co-tenancy

The co-tenancy, also called as co-residence refers to sharing of same physical resources by different cloud customers or tenants. Cloud computing provides the better utilization of resources through this concept in which different tenants may have their VMs, running in the same physical machine. It raises a serious concern about security. Such a vulnerability can be exploited in launching attacks such as VM Escape attack [48], Cross-VM side channel attack [58], etc.

Vul2 – Lack of Physical Control

In cloud computing, the tenant's data, program and their computation is outsourced to remote servers of cloud. This leads to lack of physical control on tenant's data, programs and machine, etc., which may result in dangerous attacks [59]. For example, the tenant's data residing in remote cloud servers

can be modified, leaked or even lost. An attacker can inject the malicious code in the tenant's software application running in cloud and cause harm in cloud resources. It could lead to dispute between cloud service provider and tenants. It is difficult to ensure the data confidentiality and integrity just by making use of traditional security mechanisms.

Vul3 – Under-provisioning of Bandwidth

Traditional DDoS attacks have been prevalent in cloud computing environment as well in which network layer is flooded with excessive traffic connections to exhaust the resources. In addition, a new form of DDoS, exploits the feature of under-provisioning of resources in cloud environment. In this form of DoS, shared resourced such as memory, storage and computation is consumed by attacker excessively, making the other VM users deprived from resources. DDoS in cloud, also takes the benefit of under-provisioning of cloud resources. CISCO's states that a data center design is under provisioned with a factor of 2.5:1 to 8:1 which means the network capacity of data center is less than the average capacity of hosts running in same subnet [60]. The under-provisioning of bandwidth exploited by attackers in flooding the network.

Vul4 – Pricing Model of Cloud

Cloud Computing is based on the pay-as-you-go pricing model. The pricing model is based on the computation of metrics such as bandwidth consumed, servers/VM hours, storage capacity, bandwidth, CPU utilization, etc. However, if pricing model is compromised, the billing information generated by cloud service provider will provide the incorrect information [61]. Tenants will suffer by paying for additional billing charges. One such attack is called Economic Denial of Sustainability (EDoS) attack [61] which affects the pricing model of cloud adversely.

Vul5 – Insecure Browser and APIs

Cloud vendors provide a rich software API support in order to allow customers to interact and manage with services. The APIs helps to effectively perform the service provisioning, service orchestration, service usage and service deallocation/release through web browser (client program). Any vulnerability present in the APIs can be used by attackers in breaching the security of cloud services. There are many web-based attack possible such as phishing attack, SSL certificate spoofing attack, cross-site scripting attack (XSS) and sql-injection attack, etc. [62]. Web Security standards should be followed by the APIs in order to ensure the safety of services though web-based attacks.

Vul6 – Illegitimate Access to Management interface

A management interface such as AWS management console [63], is used to manage the client's subscription for resources such as instance, storage, computation, etc. If the management console is breached by unauthorized users, it may lead to drastic consequences. Cloud environment consists of more number of users and administrators when compared to traditional computing environment. It raises the probability of gaining unauthorized access to the cloud resources through a weak management interface. Insecure cryptographic keys and algorithms can also result in such security breach. For example, Amazon EC2 management interface was breached in the year 2011 through XSS attack which exploited a cryptographic loop hole in service.

Vul7 – Insecure Internet Protocols

Any algorithmic vulnerability present in internet protocol can also be helpful for attackers in bypassing the cloud security mechanism. ARP poisoning is one such example of protocol vulnerabilities which can be exploited by a malicious VM user. A malicious user can exploit the vulnerability in re-routing the traffic of some co-located VM to malicious VM. Some other attacks which exploit protocol vulnerabilities are RIP attack, DNS poisoning attack, flooding attack, etc. HTTP protocol is also vulnerable to session-hijacking session-riding and used as web application protocol for web service running in cloud [64].

2.1.2 Need of cloud security

Cloud computing has become a successful business model because of the ease and flexibility in provisioning and managing services. However, the lack of control on data and services has raised serious concerns related to security. Therefore, there are still many enterprises who fear in migrating their services to cloud. In traditional data centers, there was a direct control on every layer in the computing stack from hardware to software. However, in virtualized data centers, the direct control is lost and complete stack comes directly under the control of cloud service provider. Hence, an organization is required to have a significant level of trust with cloud service provider before transferring services into cloud. Security has been the major barrier in adoption of cloud services over the years [47].

There are three different types of cloud service models in cloud, i.e. SaaS, PaaS, and IaaS. The vulnerabilities and security requirements for each layer varies from layer-to-layer. SaaS provisions the web-based services in most of the cases through internet. Attackers target the API interface of the web portal and sometimes the secure shell (SSH)to launch attacks in SaaS services by hijacking private keys, credentials and API keys of the tenants. The web interface can be exposed to cross site scripting attack (XSS) and signature wrapping attack [62].

Zhang et al. [65] proposed an attacking framework to launch cache-based side channel attack in PaaS cloud. The victim's VMs execution is traced by providing the extended version of Flush-Reload attack. The tenants co-location is traced first and then the private key information is extracted by the proposed attacking framework. Other form of PaaS attack targets the VM images and injecting malicious code resulting into data stealing [66]. IaaS infrastructure can also be subjected to various attacks.

The cloud infrastructure can be subjected to various malware and network attacks. For example, the virtual switch which connects the co-located VMs, can be sniffed to monitor the network traffic of co-located VMs. The virtual network can also be subjected to ARP spoofing, MAC spoofing attacks. ARP spoofing is used to reroute the traffic to malicious VM by alerting the ARP table. MAC spoofing is used to imitate another host in the same network [67]. The pricing model of cloud can also be compromised, leading to incorrect billing report generation for the infrastructure usage or software usage or platform usage.

CSP usually provides maximum access privileges of VMs to the cloud customers/tenants. A malicious tenant can attempt to gain root access of machine by installing malicious software such as rootkits. Once root access is obtained, attacker can try to breach the security of hypervisor or even the host operating system. In addition, nowadays, attackers are making the malware code more advanced which senses the monitoring virtualized environment and even the security analysis tool. On detection of the analysis environment, malware changes its behavior and bypasses the detection approach. Hence, traditional security techniques may fail to detect such advanced malware. A compromised VM can be used to launch further attacks in cloud and is a big threat to cloud. It may ultimately lead to monetary disputes between service provider and service consumers.

One of the key features of cloud is portability and inter-operability of services. However, the live migration of services can be exposed to serious security and privacy threats. Man-in-the-Middle (MITM) is one such threat in which intruder can eavesdrop the connection and mimic the destination machine [68]. The sender machine will then communicate with attacker machine, considering it as destination machine. Some of researchers, who are working in the area of cloud security, have proposed security frameworks [69, 70] to deal with security threats in cloud. However, a centralized security framework becomes a bottleneck when there is an increase in the number of TVMs in the cloud host and when the security tool uses centralized resources.

A distributed security framework that deploys the same security solution at all layers in cloud becomes less efficient because of the limitations associated with different layers. One of the security solutions could be monitoring specific security-layer(s) of cloud which will be centrally controlled and configured by Cloud Service Provider (CSP). It will enable the CSP to assign the specific security solution based on the tenants demands. In some of the existing frameworks, the security solution is deployed in individual tenant virtual

machine which will be controlled by the administrator for security reasons. The chances of subversion of security tool, in such a scenario is quite high. Moreover, the security becomes much costly as individual security daemons are developed and deployed in each of the virtual machine. Moreover, the virtual machine-level solutions cannot be directly applied to the hypervisor-layer. Research are working toward introspection approaches for providing the security from hypervisor-layer.

The shared and distributed nature of cloud is complex and prone to various security challenges. The implementation of the security solution by cloud customers is not applicable to the management level behind the virtual infrastructure. Although a service level agreement (SLA) is signed between service provider and service consumer and major security and privacy related aspects highlighted. However, there is still no standard design methodology for SLA [66]. Moreover, in present scenario, customers are still least aware about the attacking incidents and open vulnerabilities and reports. There is a strong need to work toward cloud security area to provide more efficient, transparent and distributed security solutions to deal with various cloud threats.

2.2 Cloud Security Concepts

It is important to understand some important security concepts in cloud before understanding the security solutions. Some of the important security concepts associated with cloud are multi-tenancy, virtualization, data outsourcing, trust management and meta security, etc. The details for the same are given below.

2.2.1 Multi-tenancy

Multi-tenancy enables the tenant users to share the running instances. The sharing of single cloud platform improves the efficiency of the system. In case of IaaS cloud providers, multi-tenancy refers to the sharing of Virtual Machine Monitor (VMM) among multiple VMs. In case of PaaS cloud providers, multi-tenancy allows the users to share the same developing platform such as Java Virtual Machine (JVM) and .NET platform. In case of SaaS provider, it enables the provider to share the application software among multi-tenant users. It's easy to maintain, configure and manipulate the data stored in the single database. On one hand, multi-tenancy provides above benefits to the provider; however, it also expands the threat model and can be exploited using co-residence attacks as single server is being shared by multiple VM users. Cross VM side channel attack is one of such attack which attacks the co-located VMs by exploiting information of side channels such as cache, power, heat, etc. [71]. Denial of Service (DoS) is another example that can be launched

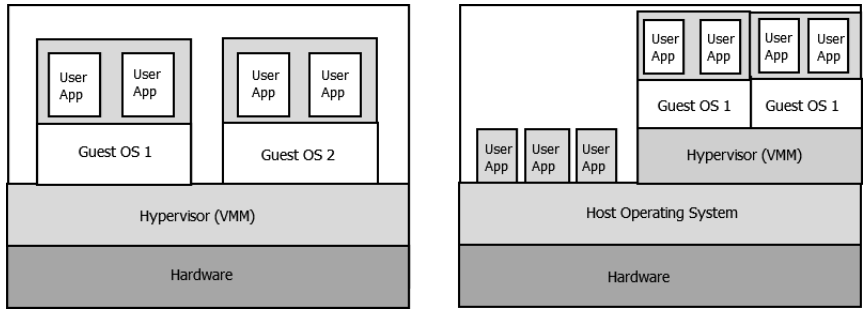

FIGURE 2.3: Types of hypervisor.

against co-located VMs very easily. VMM DoS can even consume the resources of the underline sharing platform [60].

2.2.2 Virtualization

The key technology in cloud environment is virtualization that powers the cloud environment. Virtualization enables the extraction of computing resources, services, operating system and applications from underline infrastructure on which they run. Two key components of virtualization are virtual machine (VM) and hypervisor/virtual machine monitor (VMM). A VM basically represents the emulation of the physical resources which runs an operating system called as guest OS. The emulated devices such as virtual RAM, virtual disk, virtual network interface card (vNIC) card provide the same functionalities of physical devices. A guest OS can host different applications and does not have direct access to hardware. VMM or Hypervisor runs above the hardware or software and hides the complexity of physical hardware. It allows the execution of multiple guest operating systems (OSes) in same machine. Hypervisor can easily create, delete and run different VMs having different OSes installed which is an essential requirement to provide the elastic and on-demand services in cloud computing. There are two types of hypervisors: Bare Metal Hypervisor (called Type I) and Hosted Hypervisor (called Type II), as shown in Figure 2.3. In former case, VMM can directly run on top of the hardware and access resources. Hypervisor is booted first and have access to the real device drivers. Xen [72], VMware ESX/ESXi [73] are some examples of Type I Hypervisor. In later case, it is host OS which is booted first and at the time of launch of first VM, hypervisor is loaded post-boot. The Hypervisor runs above the host operating system as a user space application. It shares device drivers from host OS to handle the input-output and completely depends on host OS for its operations. VMware Workstation [74] and Oracle Virtual Box [75] are examples of type II Hypervisor. Gradually software were developed for implementing cloud computing platform such as

Open Nebula [76], VMware vSphere [73], OpenStack [7], Citrix XenSever [72], HP Helion Eucalyptus [77], etc.

2.2.3 Data outsourcing

Data outsourcing is one of the key benefits provided by cloud service provider. It refers to the transferring of the computing, security, and especially storage to off-premise third party organization which controls the off-premise infrastructure. The capital expenditure (CapEx) along with operational expenditure (OpEx) is reduced to a significant extent. Due to outsourcing, customer loss their physical control over data which is one of the most important security issues in cloud computing. Data outsourcing also causes privacy violation as the data is outside the physical access of customers. In order to resolve this issue, customers need to be very careful while selecting a trusted service provider. Habib et al. [78] have addressed the issue of how to select a trusted service provider. A CSP should achieve the important security goals such as confidentiality, integrity and availability, etc. There are some approaches to preserve the privacy of outsourced data from outsiders. For example, Slamanig et al. [79] proposed an approach based on accumulator which maintains the Access Control Lists (ACL) having different permissions (read, write, and delete) for different users. The owner of the data can only grant/delete/modify access to the data for outsiders. In this way, unauthorized access to outsource data will be denied by the server. Another scheme called privacy-enhanced access control for outsourced data is proposed by Raykova et al. [80]. In their approach, coarse-grained access control is combined with fine-grained cryptographic access control. Adding cryptographic access control policies overcomes the trust issues with outsourced data.

2.2.4 Trust management

Trust is one of the crucial security issue concepts. It is very important for a service provider to build a trust between the tenant users and service providers. Tenant's data resides on off-premise datacenters which is completely outside the control of users. This loss of physical control raises a concern of trust on service providers. It is a multi-phased phenomenon to evaluate the trust. The security of tenant's data relies on the security management policies implemented by service provider. Tenants have to trust on them. In addition, trust on underline infrastructure of cloud such as operating system, guest OS image, hardware, application software, cloud network is another important concern for the tenant users. A trusted third-party (TTP) can authorize, audit the sensitive data of tenants and provides the security from illegitimate users. However, TTP can be compromised which leads to user's sensitive data on danger. Trustworthy systems are also discussed by Yasinsac and Irvine [81]. Tenants have to trust that systems will work fine for different circumstances such as operational error, system error, human intervention error, etc.

The trust-based systems ensure the system security as well along with the business continuity of the organization.

2.2.5 Metadata security

Cloud Organizations also maintains the massive amount of metadata which is called "data about data". It contains sensitive information in different format. For example, Web Service Description Language (WSDL) [82] is one of the examples of metadata. An attacker can exploit the WSDL and modify it. This may cause the leakage of the user's confidential data. There are some security concepts associated with it such as data sanitization, data separation, data location and data maintenance. Data sanitization refers to permanently destroying the piece of data stored in different locations in cloud. It is a irreversible process of destruction of data. During removal, some of the metadata may not fully deleted resulting data leakage of user's sensitive information. Data separation causes the tenant to use the data of his/her domain and denial of access to other domain's data. However, data separation is done in the same hard disk being shared among multiple tenants. A poor implementation of separation policy will result in data leakage. Cloud offers data migration with VMs whenever required. The mobility feature may sometime result into loss of sensitive information and also increase the chances of errors in metadata. Man in the Middle Attack (MITM) [83] is one such threat to data in transit. It may also be dangerous to keep data at multiple-locations for backup. Data maintenance is another important security concept. Maintaining the metadata along with the applications is another challenging task. Sometimes, security attacks can take place during updation of the software patches.

2.3 Cloud Security Standards

Various unwanted attack incidents happening in cloud environment, have led to the generation of security standards. Various security standards have been discussed which covers different cloud security aspects. As per the author's assessment, various cloud security standards are as follows.

2.3.1 Information technology infrastructure library (ITIL)

ITIL [84] is security management framework that identifies best guidelines and practices which defines the process-based integrated approach for managing the cloud information technology services. ITIL is applicable to all type of IT services including the cloud services. ITIL makes sure that proper security

care is take at all three levels of business operations, i.e. strategic level, tactical level and operational level. ITIL provides best practices for information security process that can be modified and used by any IT organization. A framework with continuous improvement is provided which can be aligned as per the changing need of the IT services. As cloud computing is such type of continuous changing organization. Here, the security guidelines and practices must be modified dynamically as per the business need. ITIL breaks down the information security practices into various levels:

1. Policies: The key objectives aimed by the organization to achieve. item Processes: What guidelines to follow to meet the objectives?

2. Procedures: How to distribute the activities among people and settling down the important deadlines.

3. Work instructions: What are the instructions to be performed for doing specific activities.

The key challenge faced by the organization while adapting ITIL is to redefine the set of ITIL processes that they are having efficiently. The organization is supposed to identify the gaps in the existing security processes and then mapping them as per the ITIL framework.

2.3.2 Control objectives for information and related technology (COBIT)

COBIT [85] is another security standard which is developed by international professional association ISACA which provides best practices for IT management and governance. It acts as an interface between processes and business goals. The model can also be used together with more standards such as ISO/IEC 27000 and ISO/IEC 20000.COBIT includes the following components:

1. Process descriptions: It focuses on the having a reference process model and a common language in an organization. The reference model maps the responsibility areas of planning, building, running, and monitoring.

2. Control objectives: A set of high-level requirements are provided which are to be implemented by management for having good control on IT Processes.

3. Management guidelines: The guidelines helps in measuring performance, setting up common objective, assigning responsibilities, and mapping relationship between processes.

4. Maturity models: These models are used to measure the maturity and capability for each process and identify the gaps.

2.3.3 ISO/IEC 20000

ISO/IEC 20000 [86] belongs to internationally well-known standards for IT service management not limited to cloud services. It reflects the best guidelines within ITIL. This standard is developed by ISO/IEC JTC1/SC7 in 2005. Overall, there are thirteen parts for this standard. Various requirements to establish, implement, maintain and continuously improve the service management system (SMS) are specified in ISO/IEC-20000-1 :2018. The applications of SMS as per the requirements in ISO/IEC 20000-1:2011 have been provided by ISO/IEC 20000-2: 2012. The scope definition and usability of ISO/IEC 20000-1 in applications, is being given in ISO/IEC 20000-3. ISO/IEC 20000-4 for process assessment has been withdrawn and a new series of documents have been developed by ISO/IEC JTC1/SC7. To achieve the requirements of ISO/IEC 20000-1, the best practices have been defined by ISO/IEC 20000-5. The requirements for assessment has been defined by ISO/IEC 20000-6:2017. The integration of SMS and quality management system and/or information security management system (ISM) have been defined by ISO/IEC 20000-7. The standard ISO/IEC 20000-9 has been withdrawn. ISO/IEC 20000-10:2018 defines the concepts of ISO/IEC 20000 and identifies the relationship between ISO/IEC 20000 and other standards. ISO/IEC 20000-11:2015 defines the relationship between SMS and ISO/IEC 20000-1. ISO/IEC 20000-12 defines the relationship between SMS such as CMMI and ISO/IEC 20000-1. The relationship between SMS such as COBIT and ISO/IEC 20000-1 is defined in ISO/IEC 20000-13.

2.3.4 Statement on standards for attestation engagement (SSAE)

SSAE [87] is standard developed specially for auditing tasks which is applicable to cloud service providers as well. The total 16 audits come under one of the three classes of Service Organization Controls (SOC): SOC 1, SOC 2 and SOC 3. SOC 1 focuses on financial reporting control. SOC2 assesse the security control of technical and operational tasks and defines the trust services principals for them. SOC 3 ensures and reports whether the service provider is meeting the principals of trust services. The reports generated by SOC3 are freely distributed. NIST provided a Cybersecurity Framework (CSF) which focuses on applying the federal security assessment and security authorization controls in industries owning their own infrastructure. CSF is a standard security framework for private cloud service providers.

2.3.5 Cloud security alliance (CSA) cloud controls matrix

CSA [88] provides the guidance for ensuring the cloud security and provides the certification for same in order to promote the security enabled delivery of cloud services. A Cloud Controls Matrix (CCM) has also been published

by CSA that provides the description of key security control which can be used to assess the services of cloud providers. This is very useful document that ensures the effective implementation of the cloud security governance. CCM provides guidance in 16 domains of security including identity and access management, application security. Key management, mobile security and data center operations. The 16 domains primarily focus in three areas of cloud computing: Architecture, Governance and Operation in Cloud Computing. A baseline is set by the CMM for helping organizations to achieve best cyber security strategies. Customers can use CCM metrics to compare various cloud service providers. By following CCM, organizations are preparing themselves to follow other standards such as HIPAA, NIST, ISO 27001, HIPAA, etc.

Security frameworks explained above such as ITIL, ISO/IEC 20000, and ISO/IEC 27001/27002 security frameworks focus on:

- Ensuring that current security policies are according to the need.
- Applying the security baseline in all IT operations.
- Ensuring that all the services are secure from cyber threats.

Incorporating these frameworks in the organization impact the organizational growth and reduces the risk from outsider threats.

2.4 CSA Cloud Reference Model

The cloud security reference model [89] addresses the relationships of different cloud stakeholder classes. As per the security control and concerns, each of them is placed in the architecture. The following need to be known for avoiding confusions in services:

- The term how cloud services are deployed is completely related with where the cloud services are provided. The description of public or private cloud can be done as external of internal.
- It is very important to understand the security boundaries of the organization who should have to follow a well-demarcate perimeter as security perimeter. Cloud services are consumed in the manner of the location of security perimeter of the organization.
- The deployment and consumption of cloud is not only related with the location (internal or external) of cloud services but also related with physical location of resources and who consumes the resources who is responsible for security, governance, policies and standards.

In addition, the location of assets, the security risks are also associated with followings:

- Who is responsible for managing assets and how assets will be managed.
- Which type of assets, information and resources are being managed?
- What are the controls being selected and how they are integrated?
- What are compliance issues associated with services?

Infact ISO/IEC 27002 says that the introduction of external third parties or services should not affect the organization's information processing facilities. There is a difference in the responsibilities and methods for securing different cloud models. It raises various security challenges with customers. Cloud customer can only be aware about the type of security controls and at what level they are implemented if the cloud service provider (CSP) share such information with customers. The customers can be tremendously misguided for making risk management decisions without proper awareness about the security controls. CSA cloud security architecture maps the cloud model with the security controls as shown in Figure 2.4 [89]. Once the mapping is done, it becomes easier to determine what needs to be performed to feed back the risk assessment framework. It helps in deciding how the risk should be addressed,

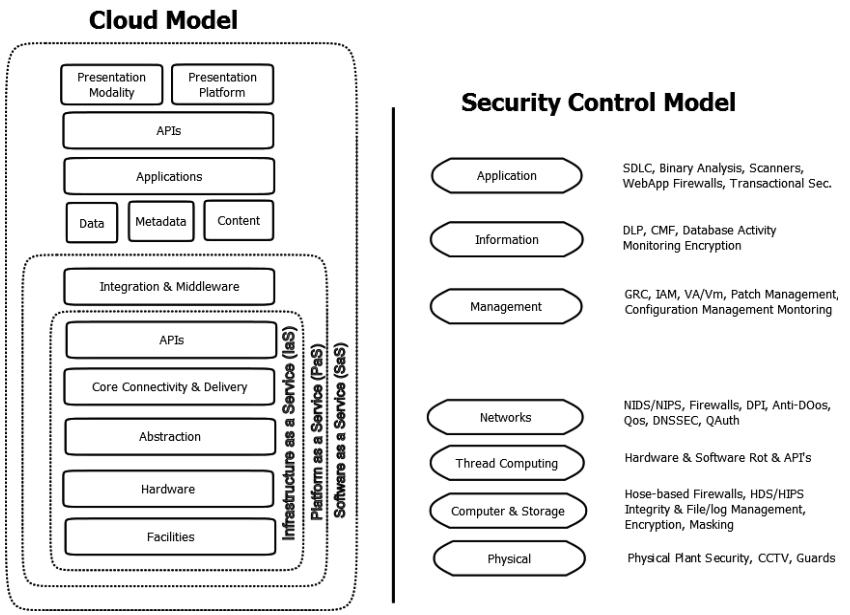

FIGURE 2.4: CSA cloud security reference architecture.

accepted, transferred and mitigated. The gap analysis maps the cloud services and classifies them against architecture model. As an output of this gap analysis, general "security" posture can be determined and can be related to the asset's assurance and protection requirement. It then becomes possible to map the security architecture with regulatory, business and other compliance requirements.

The security controls in IoT are quite similar with the security controls in IT environment. However, because of the various types of service models, operational models and technologies used by cloud computing, there are different risks associated to an organization in cloud environment than traditional IT environment. The security controls are implemented at various layers such as physical security layer, network infrastructure security layer, IT system security layer and information/application security layer. In addition, security controls are implemented at people and process level like assigning different roles and responsibilities and change management, respectively.

The security responsibilities vary for both service provider and service consumer for each of the cloud service models. For example, let's consider the example of Amazon's AWS EC2 service which is IaaS service offered by Amazon. With respect to this service, the service provider is responsible for the security controls such as securing the hypervisor (virtualization-layer), physical security and environmental security, etc. The service consumer will deal with the security controls such as instance security such as security of applications, operating system and consumer's data. However, for SaaS service models such as Salesforce.com's customer resource management (CRM) which deals with the entire stack. The provider not deals with security control of environmental and physical security but also deals with security controls for applications, data and infrastructure. This reduces many of the responsibilities of cloud customer related to directly handling the security controls.

Presently, there is no provision for the consumers to understand for what are their responsibilities for ensuring security. However, CSAs are making efforts to define standards in cloud audits. The cost efficiencies supported by providers are one of the major focuses of attraction of cloud service provider. The efficiencies are provided by making the services flexible so that a large number of customers can takes its benefits. It is not fortunate that solutions integrated with the security are not perceived flexible. The rigidity often comes because of the abstraction in the infrastructure and lack in the visibility which often makes it difficult to integrate the security controls specially at the network layer.

In SaaS environment, the negotiation of the security controls with their scope is done in service contracts. The privacy, compliance and service levels issues are handled legally in service contracts. However, in IaaS services, the key responsibility of securing the underline infrastructure is of service providers and the remaining cloud stack is the responsibility of the consumers. However, In PaaS services, the provider is responsible for securing the platform. The consumers are responsible for developing the applications in a secure

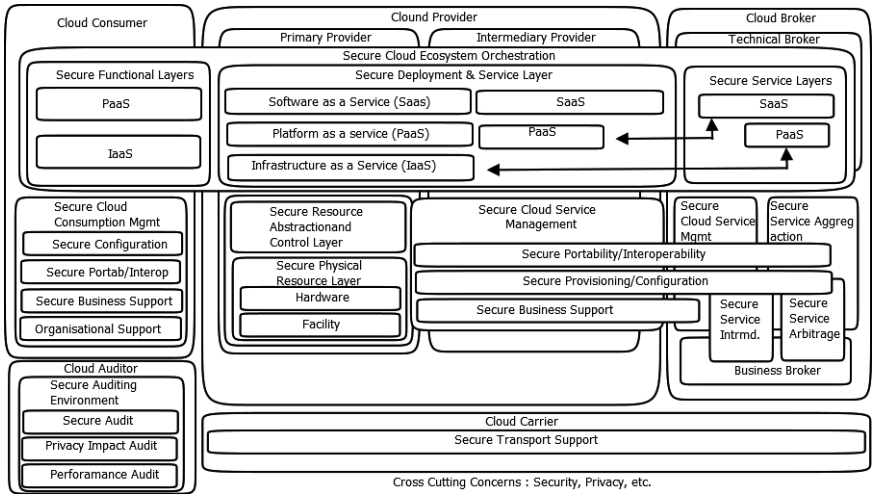

FIGURE 2.5: NIST cloud security reference architecture.

way including the security of the developed applications. It is very crucial to understand the difference between the security control with respect to each service model in order to deal with the risks associated with organizational operations.

2.5 NIST Cloud Reference Model

The formal model of cloud computing security reference architecture (NIST SRA) has been derived from NIST reference architecture (NIST RA) as shown in Figure 2.5 [90] which depicts various architectural components. The architecture depicts that the components identified by NIST RA, should be safe. The ultimate aim of cloud customers is to find out the security controls which best fits the security needs of customers. The ordered list of all the architectural components and sub-components are described as follows:

2.5.1 Architectural components of consumer

The cloud customer's responsibilities were not explained in earlier architecture NIST RA. However, NIST SRA provides the detailed description of the cloud customer's architectural components. The architectural components of consumers are described with their sub components on the following pages.

Secure Cloud Consumption Management

This component includes functions which are very important for the operations of services used by consumers. The various sub components are

i Secure Configuration: It is responsible for the secure management of the following areas: rapid provisioning, resource changing, monitoring and reporting, metering, service level agreement management.

- Rapid provisioning: It refers to automatic deployment of cloud services and resources in the cloud systems. The secure provisioning of resources ensures that the requests are coming from the authorized and authenticated sources.
- Resource Changing: It refers to doing the configuration changes, upgrades and resource reassignments/release, etc. in the cloud environment. The secure resource changing ensures that only authenticated and authorized requests for resource are considered.
- Monitoring and Reporting: The virtual resources are monitored and reports are generated in some time intervals. The secure monitoring and reporting ensures that the limited/required use of resources.
- Metering: It refers to the billing facilities provided by service provider to generate bills based on the usage of resources. The secure metering refers that the pricing model should not be compromised by attacks such as EDoS.
- Management of Service Level Agreement: It refers to managing the SLA definitions, monitoring, and policy enforcement. The secure SLA management ensures the visibility of clauses with customers.

ii Secure Portability/Interoperability: It makes sure that data can be moved securely to various cloud environments. The components mapped to this sub-component provide higher flexibility for the security of data which is being transferred to the different cloud providers. The data security and protection scheme are enforced to mitigate the risks. A greater amount of flexibility is provided for securely transferring data/applications over another cloud provider's platform by incorporating security components at this level. However, there are many other challenges other than security while supporting data migration. Providers are working in this direction to support interoperability feature to students via secure channel. The basic requirements for supporting such as feature varies service model to service model.

iii Secure Business Support: It includes services used for running business operations like management of service contracts, payment, business relationships with other cloud actors and many more, as listed briefly:

- Cloud actors such as Broker, Auditor and Carrier are managed at this level along with their business relationship. The interaction between the cloud actors is formally authorized and authenticated as per the security guidelines.
- Business Issues and other problems related to cloud are discussed with the actors identified for organizations' cloud ecosystem. The best security practices are discussed to ensure the business continuity.
- The service contracts are managed to ensure the secure set-up of contracts, secure termination and closing, etc.
- Only those services are procured where security concerns have been addressed properly.
- The payment and invoices are also managed securely by following best security practices to avoid any fraudulent transaction.

This architectural component also includes various other features such as provisioning of identities and credentials to the employee of organization and contractors by applying access control policies and business continuity plans.

iv Secure Organizational Support: It is responsible for covering processes, policies and procedures given by an organization to support the overall secure consumption management of cloud. The compliance management, audit management and the governance risks and compliance, the standards related to technical aspects, policies and standards for information security, etc., are sub-components of this architectural component.

Secure Functional Layer

The components are used to secure the cloud functional layer and rely on the particular cloud service model used. The modules of this layer are:

First is SaaS cloud ecosystem, in which cloud consumer only has limited administrative control of applications. In another way, it can be said that minimal access control in cloud and security components are provided. Second is PaaS cloud ecosystem, in which cloud consumer has the control on applications. In addition, some control is also given for the hosting runtime environment. However, there is no or limited access to the infrastructure such as access to network, server and storage.

Lastly, third is Iaas cloud, in which cloud consumer has some control in the provisioned infrastructure mainly, virtual machine, middleware and guest OS. The access to virtual computing resources offers more privileges to the users than other service models. However, access to host or physical server and hypervisor is still not granted. For example, a cloud customer can implement a security system such as firewall to secure the infrastructure allocated to it.

The access control policies are specific to a service model. The details about access control, rules, policies and standard is clearly specified in the SLA.

2.5.2 Architectural components of CSP

Various activities are carried out by the service provider such as coordination, management of the resources, etc. A proper ecosystem need to be managed for the provisioning of secure cloud services at various levels such as SaaS, PaaS, and IaaS. The sub-components are as follows:

Secure Cloud Ecosystem Orchestration

Cloud provider performs the functions of orchestration of services, management of services, privacy and security aspects. By NIST, it is described as the composition of various design components that supports which help the provider in coordinating and arranging the cloud components. It has the following components and sub components, as follows:

i Secure service and deployment layer: The requirements of security components depend on the type of service offered to the customers. In case of IaaS cloud, the cloud provider has full control on all the infrastructure resources such as physical server, networking resources and storage. It also executes the management software for accessing the hardware and has full control on it. The cloud consumers are offered the access of virtual resources such as virtual machine, virtual network, etc.

ii In case of PaaS cloud, cloud service provider handles all the computing resources and facilitates the middleware and runtime execution environment. The PaaS ecosystem offers all development tools and/or infrastructure to the customers. PaaS customers have certain control the development tools and deployment infrastructure. In case of SaaS cloud, the provider has complete control on full stack and handles the maintenance, configuration and updation of applications as well. Service provider provisions the services to customers in SaaS ecosystem for effective usage. Customers have limited control in the application only.

iii Secure abstraction of resources and control layer: It represents the security components which a CSP would implement in order to provision the safe access to the physical components. It is the responsibility of the service provider to ensure that proper security processes and components are in place to enable the legitimate access to the resources. The data owned by one tenant should be safe from other tenants sharing the resources. The data of one user should not be accessed by other users. The non-privileged users should not be allowed to access the service management related functions.

iv Secure physical resource layer: The physical resources such as Memory, CPU and networking resources (firewall, router) and storage devices (Hard disks, etc.), should also be secured from the unauthorized access. This layer facilitates such security components which ensure same. The other

resources such as ventilation, heating, communication and power are also included at this layer.

v Secure cloud service management: It has been described with the perspective of requirements as follows:

a Secure provisioning and configuration : It provides the following functionalities:

- Rapid provisioning: The services are provisioned and deployed automatically on receiving the service demand from the customer.
- Resource updation: It refers to upgrading and maintaining resources as per the modified security policy.
- Resource Monitoring and Reporting: Cloud virtual resources and cloud events are monitored and security reports are generated which also comprises of resource usage statistics.
- Metering: The billing facility is provided with some abstraction based on the service type (processing, storage, etc.)

b Secure interoperability and portability: It provides the assurance that the customer's data can be easily transferred securely to various cloud ecosystems as per the requirements of security as identified by SLA. The maintenance time and downtime should be fixed at minimum level.

c Secure business support: It comprises of business related services which supports the security processes of customer's and provider's. For example, contract management, customer management, inventory management and reporting and auditing, etc.

2.5.3 Architectural components of broker

The services defined for cloud broker can be classified into following categories:

i Secure Service Aggregation: The multiple services are combined, forming one or more service platforms. The secure movement of data and its integration is also the responsibility of the broker. The various key sub functions are: secure configuration and provisioning and secure interoperability and portability.

ii Secure Management of Cloud Service: Various security functions which are required for the secure management of various services are included here. Sub components derived from the activities of this component includes secure portability for supporting secure transportation of services, secure provisioning of resources, tools, etc. and secure business support.

iii Secure Service Intermediation: It addresses the brokers responsibilities for ensuring the capabilities added to existing cloud services.

iv Secure Service Arbitrage: The secure service aggregation and service arbitrage are very similar in various aspects. However, in later, the combined services by broker are not fixed and are flexible. They can be assigned to multiple vendors dynamically. All the functionalities of the broker has been specified and explained above. Broker is supposed to perform all its functions, considering in mind the security requirements specified in SLA.

2.5.4 Architectural components of carrier

The transport and connectivity of the services is provided by the actor. The secure management of services is also performed by the cloud carrier in order to ensure that customer satisfaction about the service delivery is maintained. The cloud carrier provides the way via which cloud customer can directly contact the broker or provider. The complex details in order to maintain the connectivity is concealed from the consumer. Although carrier plays an vital role and makes it possible to have a transportation of services between provider and consumer without having a cloud carrier. Cloud service provider ensures that a secure channel should be provided to cloud customers to meet the SLA requirements which are signed between them. In addition, service management functions are also performed by the cloud carrier to ensure the effective service delivery to the customers.

2.5.5 Architectural components of auditor

Cloud auditor is responsible for performing the independent assessments of the services. It ensures that system operations, security policies, privacy functions, etc. are properly functioning without compromising any service quality. The secure auditing environment includes various mechanisms such as security controls, secure archival, secure storage, data location, metering, SLAs and privacy, etc. It requires the following security mechanisms in place

- Secure Archival: The archival of all the audit records for the business and legal processes should be secure. The requirements for archival and its implementations should be available to auditors.
- Security Component and Related Control: The detailed information about the various security controls and security components should also be available to auditors.
- Secure Storage: The evidences can be collected from concerned authorities and stored in cloud safely for future purpose. Therefore, the secure mechanisms such as obfuscation and encryption information should be provided to the auditors.
- Data Location: Some jurisdictional rules might be required to be applied in data during the process of assessment. It requires the availability of information about data location to auditors.

- Metering: The metering/billing information need to be given to auditors for the performance audit. The access should be granted in secure manner.
- SLAs: Auditors are also required to have a secure access to the all the agreements which are implemented between the parties.
- Privacy: The privacy assessment by auditors also requires the secure access to the information about the configuration information and system security which are implemented by organization for protecting the client's data.

The security controls along with the security components are independent of the cloud service model and available to all the cloud auditors.

2.6 Conclusion

Cloud Security plays an important role in building a trust between cloud service provider and cloud consumers. It provides tools and technologies to protect the infrastructure, applications and data. Various security aspects for cloud are same as the on premise organization. However, the addition of virtualization layer has opened the doors for attackers and hence requirement for specialized security techniques to deal with cloud specific threats. Various cloud security concepts have been discussed such as multi-tenancy, virtualization, data outsourcing, trust management and meta security, etc. Afterward standards for cloud security have been described such as Information Technology Infrastructure Library (ITIL), ISO/IEC 20000, Statement on Standards for Attestation Engagement (SSAE), Cloud Controls Matrix and Cloud Security Alliance (CSA), etc. A cloud service provider has to follow the security standards in order to maintain the security of organization and customer' data. At the end, some of the important cloud security reference architecture (such as NIST, CSA) have been discussed to provide an overview about security architectures in cloud.

2.7 Questions

Fill in the blanks

1. Which of the followings are cloud security standards

   i ITIL

ii COBIT
iii ISO/IEC 20000
iv All of above

2. Mark the appropriate sentences. The security risks are associated with

i Who is responsible for managing assets and how assets will be managed?
ii Which type of assets, information and resources are being managed?
iii What are the controls being selected and how they are integrated?
iv What are compliance issues associated with services?

Choose the correct option for answering the question 2.
(a) i (b) iii
(c) ii (d) all mentioned above

3. Type-1 hypervisor(s) is/are

i Xen
ii VMware ESX/ESXi
iii Hyper-V
iv All of above

4. Which are the key vulnerabilities in cloud environment

i Lack of physical control
ii Under-provisioning of bandwidth
iii Pricing model of cloud
iv Insecure Browser and APIs

Mark the correct option for answering the question 2.
(a) i & ii (b) iii & iv
(c) ii & iii (d) all mentioned

5. Mark the incorrect statement. The attacks which exploit protocol vulnerabilities and affect pricing model of cloud are

i RIP attack
ii DNS Provisioning attack
iii Flooding attack
iv Economic denial & sustainability attack

Short-Answer Questions

1. Explain various functionalities of auditor with associated security concern.
2. What do you mean by cloud security standards. Explain COBIT.
3. What is ITIL standard? How does ITIL help in meeting the security requirements?

Long-Answer Questions

1. Define Cloud security. Discuss all the architectural components of NIST cloud security reference architecture with suitable diagram in detail.
2. Explain various cloud vulnerabilities. Also discuss the need of cloud security. How cloud security is different than traditional security environment.

Chapter 3

Cloud Security and Privacy Issues

3.1 Introduction

The emergence of various cloud-based services has opened good opportunities in various domains such as Internet of Things (IoT), Smart Grid, Healthcare, Banking, and IT. However, security is one of the crucial aspects in the cloud computing, which has been studied in detail by cloud service adopters, researchers, and security professionals. Cloud offers various good features for the better utilization of the resources. Many of such features have been discussed in previous chapters. However, various features such as multi-tenancy and online access to data and applications from anytime and anywhere expose some serious threats as well.

For example, multi-tenancy could be misused by some of the cloud tenants to cause harm to the shared cloud resources and breach the security of co-located VMs. Moreover, the availability of services can also become threat to the cloud infrastructure as services are provisioned in online mode. Advanced attacks can eavesdrop the network connections and can gain access to the information being shared between sender and receiver [60]. Moreover, the data stored in the cloud storage servers can also be exposed to third party organizations intentionally for gaining some financial benefits. Since the data is stored in the shared storage resources. If proper isolation of virtual storage volumes is not maintained in the physical storage, then it will be easy for an attacker to access the data of other customers.

Furthermore, the vulnerabilities present in any component of the cloud infrastructure such as controller server or computer server, network server, hypervisor, virtual machine and user applications, etc., impose a direct threat to the security and privacy of services. Some of the other vulnerabilities which can hinder the security and privacy are: insecure live migration of the customer's data, random selection of cloud service provider, in secure application and browser APIs at provider end, network vulnerabilities and insecure encryption of data, etc. [91]. The vulnerabilities and threats present in cloud, make it very difficult to develop a comprehensive security model that can cover all possible vulnerabilities.

Due to some security reasons, cloud service providers do not allow the cloud customer to impose their own security model at the cloud network, or

DOI: 10.1201/9781003004486-3

integrate them with management services or API, etc. It is the responsibility of the provider to secure each layer of cloud infrastructure. The customers can however install some security tool inside their own VM for the analysis of their own VM's activity. If the VM is subverted, the security tool inside VM will also be subverted. Therefore, security and privacy are major concerns for cloud service vendors and end users before migrating their applications, data or any services in cloud.

Security refers to the protection of cloud infrastructure along with associated data and applications from the unauthorized threats and attacks. The protection of cloud resources is important to ensure the confidentiality, integrity and availability (CIA) in cloud environment. For example, the unauthorized users should not be allowed to access and modify the cloud resources. The services should be available anytime from anywhere and service outage should be as minimum as possible. The user's data could be very sensitive and protection of data from the attackers is the responsibility of the cloud service provider.

Privacy is one of the important rights of a person to not to share his private data to public. Private data refers to the personal sensitive information of person which he or she may want to share to restricted number of people or with no one. In the context of cloud computing, privacy can be defined as "the obligations and rights of an organization and individuals with respect to the gathering, usage, retention, disposal and disclosure of private information" [92]. The privacy concerns are also different for each cloud models. The security concerns for public cloud are much higher than private clouds or hybrid clouds. As publically cloud can be accessed by anyone over the web and hence more prone to security attacks. However, in private cloud, the resources are shared mainly by organizational people and attacking risk is less due to having restricted and controlled access to the resources.

Although security and privacy are defined in different ways. However, they are highly related with each other. The security is a much broader term which is used to ensure various security aspects, mainly confidentiality (unauthorized disclosure) , integrity (illegitimate modification of data) and availability (smooth access to services) of services. Whereas privacy is mainly concerned with the ability of an individual to seclude their information from public and share with selective people based on personal choice. Various privacy preserving security frameworks [93, 94] have been introduced to preserve the privacy of individuals and at the same time meeting other security goals of cloud. Therefore, security is not privacy but techniques used to ensure that privacy and others security factors such as CIA, are persevered in cloud.

However, there exist less transparency when we talk about attacking incidents and corresponding security measures taken by vendors, in cloud environment. If some security incident occurs, customers may not be aware about same. In fact, the detailed report about the incidents such as vulnerabilities exploited, malware details and any system damage, etc. is also not shared with the customers. For example, there exist some backdoor attacks which

are launched by attackers to again access to the VM instances running in cloud. The detection and notification of such backdoor attacks is essential to have in the primacy stage. However, as long as no such backdoor is reported by provider, customers are still blindly trusting the provider's security and assuming that no such attack has happened. Although the security and privacy related aspects and services are usually highlighted in the Service Level Agreement (SLA). Various popular cloud companies such as Google, Amazon, Salesforce, etc. are dependent on detailed SLA to ensure the customers that strong security is provided. However, there exists no one standard for designing the SLAs.

Various cloud features also expose threat to the security and privacy of the user's personal information and cloud infrastructure. Handling and addressing all possible security issues at all possible layer in cloud is still a challenging task. Gradually, the enterprises or cloud service providers are expanding their cloud services and hence the attack vector associated with various services is also expanding. Each of the organization is interested in incorporating a security framework for running the services in a protected environment. Moreover, the security and privacy of the user's data is as important as the infrastructure security. Each organization has to take care of choosing a secure cloud computing platform before migrating their services and data to the remote cloud servers.

3.2 Cloud Security Goals/Concepts

Cloud security is one of the essential need of today' eras as most of the organizations are moving toward the adoption of cloud service platforms. There is a strong requirement of having the proper controls, security policies, defensive mechanisms, and procedures in place so as to protect complete the eco-system. In this section, we will understand, various cloud security goals that every organization wants to achieve.

3.2.1 Confidentiality

The confidentiality of data is a crucial issue when extremely sensitive data is outsourced to the cloud system. It keeps the data secret from the users in the cloud and the confidential data must not be accessible to an unauthorized entity. To achieve confidentiality, mechanisms such as cryptography and isolation has been adopted by cloud vendors. Encryption mechanisms such as triple Data Encryption Standard (DES) or Rivest, Shamir, Adleman (RSA) are used to gain confidentiality but key management or key distribution is the big issue. Some examples of threats to confidentiality are insider user threats such as malicious cloud provider users. Malicious cloud user and malicious

FIGURE 3.1: Cloud security goals.

third-party user. The attacks by external attackers such as the attack on application or infrastructure by remote software or hardware. Data leakage is another threat to the confidentiality.

3.2.2 Integrity

Data integrity is the basic task that verifies the data and it provides the guarantee for the exactness and quality of the data. It is important as the cloud provides various services such as SaaS, PaaS, etc. The cloud services demands have been increasing day-to-day, hence cloud service providers may require increase storage. So, there are chances of data corruption or loss or maybe the cause of failure of nodes, physical devices, or disk. The data integrity is preserved in the cloud environment by various means so that data are not be altered by an unauthorized entity. To avoid data corruption or crash in the cloud, so watching the data integrity is very essential. As cloud-based environments are distributed so it is harder to obtain integrity as compared to the centralized environment. Examples of threats to integrity like user access, data segregation, and data quality.

3.2.3 Availability

In the cloud-based system that includes application and infrastructure, the goal of availability is to provide the services to its users from anywhere and at any time. But some circumstances occur in which the availability of data cannot be sure. There may be unavoidable circumstances such as natural tragedies, hence it is essential to know the data can be used, authenticated, or restored by the data users. The cloud users must know about the security actions that are to be taken by the CSP and must read the Service Level Agreement. The availability of cloud services is obtained by using fault-tolerant systems in the cloud environment that can tolerate the failure of the server or

cloud. Redundancy and hardening are two mechanisms that can be applied to increase the availability the services in the cloud-based system. Threats to availability such as the denial of services like network DNS, data, and application. Liu [95] discussed a novel cloud Denial of Service form. The effect is normally reliant on existing, processing capacity, memory, and bandwidth in flooding attacks.

3.2.4 Authentication

Authentication is the method of creating assurance in the identities of the user. Authentication guarantee levels must be suitable for the application sensitivity and information resources accessed. An identity management schemes can be used to authenticate users and cloud services using credentials. A big challenge related to Identity Management (IDM) in the cloud is interoperability limitations. Password-based authentication techniques have a genetic drawback and have important risks. The IDM must secure sensitive and private data concerning to users. As cloud service providers have been increasing day by day they support a standard SAML that is used to authenticate the users before administering the data and application access. SAML offers mechanisms that exchange information among cooperating concerns. The request and reply messages of SAML are mapped on SOAP that uses the XML format. Chow et al. [96] discussed that authentication is needed before offering access to Software as a Service application is beneficial due to centralized monitoring.

3.2.5 Authorization

The sensitive information and services of the users can be accessed by unauthorized users. To restrict data access authorization must be used. The identity management system should be employed. Authorization is used to control the access of data. Authorization is the method that allows a system to regulate access level to a specific authenticated user. There are benefits of centralized access control and alleviate many security and management actions. Though that cannot be desirable in a case populated with data mix-up, that can be happened in the future [96]. This is risky to gain access te sensitive information when authorizing third party service. Grobauer et al. [91] recognized faulty or unsatisfactory authorization tests as expected vulnerable vectors.

3.2.6 Auditing

Auditing is the monitoring task to know what is going on in the cloud-based system. An additional layer can work for audibility in the virtual machine to monitoring the system. As it can monitor the complete access duration, hence it is safer than that is made in software or applications. Audit approaches investigate service conditions, monitor malware, accesses, and other actions,

and record logs with an exhaustive explanation of what occurs are appropriate. The audibility simplifies the method of recognizing the authorized party legal action situation that can be important to the cloud stakeholders. Auditability contains in acting tests series to discover if all suitable implementations conform. In cloud environments, the other layer above virtualized guest operating systems will also agree that [97].

3.2.7 Access control

To minimize the security risk, access control features can be used that maintain the control on access to the resources. Access control is part of identity management. The eXtensible Access Control Markup Language (XACML) is the standard that can be used for resource access control in the cloud environment. XACML focus on techniques to take authorization decisions that complement the focus of the SAML on the resources for carrying the decisions of the authorization and authentication among cooperating domains. The protocols or transport methods are not provided by the XACML and it also does not describe the method of validating the credential of the users. The transmission of the message among XACML units is vulnerable to attacks that can be performed by malicious third parties such as replay, unauthorized expose, loss, and alteration attacks.

3.3 Cloud Security Issues

The rapid growth of cloud services and increased demand in the organizations, have raised various security concerns. If there exist any flaw in the implementation of any cloud service, it could be a big threat which could raise serious security issues. The migration or transitioning of services to public cloud environment also causes the transfer of responsibilities to service provider to protect the data, applications, information and infrastructure, etc. It removes the direct control on the cloud resources and management operations from the customer side. This makes the customers highly dependent on the cloud vendor for the smooth functioning of services. Various security critical operations like incident response, auto-updation, continuous monitoring of services, etc. are now performed by cloud vendors. Hence, cloud customers have to trust on the clouds vendors. However, it has been reported by various organizations such ENISA [49] that insider threats can also cause major harm to the cloud resources. The 65% of insider threats can harm the reputation of an organization and can affect the finances. Since, the customer's data is in remote servers, which is sharing its resources with other customers, the data breach can also occur from the outside personnel. Although there exist various protection laws and regulations which provides the guidelines for joint

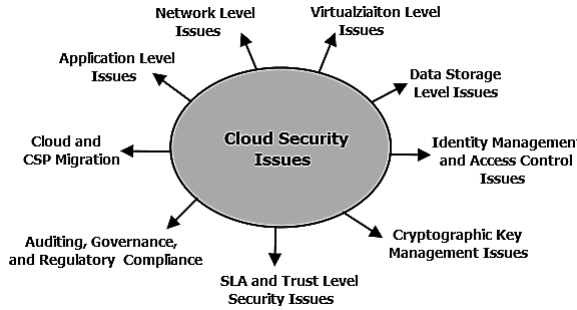

FIGURE 3.2: Cloud security issues in cloud.

responsibilities so that proper cooperation between cloud vendors and customers can be achieved.

However, due to lack of physical contact with the servers and cloud personnel, its again challenging to enforce such guidelines. There are various cloud security issues at each of the layer of cloud environment. These are application level, virtualization level, network level, data storage level, cryptographic key management level, identity management, and role-based access control, SLA and trust level, auditing, governance and regulatory compliance and cloud and CSP migration level security. Application level security issues are concerned with the vulnerabilities and threats present in the web applications, web browsers and application layer protocols, etc. Network layer security issues are concerned with the security vulnerabilities present with network layer protocols, network servers, networking applications and services and any attacking study that is targeted through network.

The virtualization layer security issues are more concerned with the threats and vulnerabilities associated with the virtual machines and hypervisor. The data storage level security issues are concerned with the storage layer attacks and vulnerabilities that can be exploited by attackers. The cryptographic key management is more or less concerned with the key management schemes and their limitations. The identity management and role-based control issues are mainly associated with vulnerabilities in customers' identity schemes and granting the resources to them. The SLA and trust level issues talks about the flaws present in the implementation of same. The auditing and regulatory policies are also major security threat as improper implementation of same, can cause severe security breach. There are various security issues associated with live migration of cloud services as well. Let us discuss each of the security issue one by one. These issues are also shown in Figure 3.2.

3.3.1 Application level security issues

Application level security issues are concerned with the security of web applications running in the cloud to provide cloud services. The SaaS application

has to be managed over the web (using a browser). The web application security is tightly coupled with the security of web browsers. A web browser is a platform independent program, used to access the cloud services (SaaS), web 2.0 or web pages. A web browser uses SSL/TLS protocol for secure transmission. The security loop holes in the web applications create the vulnerabilities in the SaaS applications. The web applications are prone to a number of threats such as cross-site scripting (XSS), SQL injection attack, broken authentication, insecure transport layer protection, cross-site request forgery (CSRF), etc.

The security at the application level states the use of software and physical resources for protecting applications such that the adversary cannot gain control over applications. Application-level security issues are concerned with the security of web applications running in the cloud to provide cloud services. The SaaS application has to be managed over the web (using a browser). As software-as-a-service and web applications are tightly-coupled with offering services, cloud services availability and protection rely on Web browsers and APIs security. A Web browser is a platform-free client program by which clients can access the SaaS and web applications. The protocols TSL/SSL can be used to authenticate and protected data transfer. It uses SSL/TLS protocols for secure transmission and authentication of data. The web applications are prone to several threats such as cross-site scripting (XSS), SQL injection attack, broken authentication, insecure transport layer protection, cross-site request forgery (CSRF), etc. Hence, the adversary can breach the security of cloud applications when they target Cloud authentication based on the browser. Any adversary can gain access to XML tokens that are authentication-related passes of another customer that is helpful to get access services of the target. The XML encryption and XML signature is the useful mechanism to improve the security of the browser [64]. Though, the XML Signature Wrapping attack allows the adversary to modify the content of the signed portion and invalidating the signature is not included. Some AWS accounts may be taken over due to the cross-site XSS scripting vulnerabilities that may be the cause of the XML signature wrapping attack.

3.3.2 Network level security issues

Network level security issues are concerned with the security of the cloud network. One of the key issues at network level is unavailability of services. Denial of Service (DoS) and Distributed Denial of Service (DDoS) are main threats to service unavailability. These attacks cause inconvenience to customers and prevent their access to the cloud services. HTTP-based and XML-based DDoS, are called as Economic Denial of Sustainability (EDoS) which affect the pricing model of cloud [98]. The key security issues at the network-level are authorization, authentication, intrusion detection, vulnerability assessment, session hijacking, etc. Some common attacks at network-layer are sniffing, scanning, IP/MAC spoofing, and DNS poisoning, etc.

The authorized clients of cloud who may be inside network adversary and they can gain access the resources of the other customers. The internals is privileged and they have more information than the external adversary. This information is important to know about the network, security approaches, and resources. Hence, this is convenient for an internal to perform the attacks than external adversaries. The key security problems at the network level are backdoor attacks, Internet protocol vulnerabilities, session hijacking. Many cloud service providers such as Azure, Amazon, etc. use a firewall to cope up with few challenges at the network level, but it cannot be helpful for inside attacks. Some challenges can be solved using integration with network-based IDS. Though, a network-based IDS must be set up for sensing not only external but also internal intrusions. This must also be proficient in sensing intrusions from encrypted traffic.

3.3.3 Virtualization level security issues

Virtualization level security issues are concerned with security of virtualization layer. The major vulnerability is the multi-tenancy in which multiple tenants share and utilize the cloud platform [60]. As the number of TVMs running above Hypervisor increase, the security issues with the new TVMs also increases. Maintaining the security policies of all TVMs is challenging task. Malicious code running inside a TVM may try to gain root privilege of the Hypervisor with an intention to take full access of the system. Security of TVMs is one of the crucial concerns in the cloud environment. Once Hypervisor is compromised, all TVMs running on it will be under the control of the attacker [99]. Infact, an improperly configured Hypervisor can fail to provide proper isolation among TVMs, leading to disclosure of the tenants' sensitive data.

When more virtual machines are added to the hypervisor, the security concern with new VMs increase as this is impossible to keep up with all virtual machines. Therefore, it is hard to maintain the security of those VMs. There may occur that a guest VM attempts to execute a malicious code on the host to gain full control of the system so that other VMs access could be blocked. The physical infrastructure is shared among multiple clients and if one user is malicious, then he can be a threat to other users who are sharing the same infrastructure. If an attacker can gain control over the hypervisor, he can modify any guest operating system and gain control over the contents moving through the hypervisor. The attackers can exploit the vulnerabilities of the hypervisor and get control over the virtual machines. Some examples of attacks are Subvit, DKSM, and Bluepill that are still an open challenge.

3.3.4 Data security

Data security is vastly an open research area. Data can be in transit (communicated via network channels) or in rest (stored in data centers). The

vulnerabilities in the network protocols and/or poor encryption directly affect the confidentiality and integrity of data. The data stored in the servers needs to be physically and logically segregated and have control policies. A few years back, Amazon reported that its Elastic Block Store (EBS) volumes were trapped which affected its EC2 instances [100]. During data-in-transit, the attack in the network will affect data integrity and confidentiality. The major risks in the case of data-in-transit can be network protocols and bad encryption approaches. Data linage refers to trace the path of the data and this is essential for auditing in the cloud. This is a critical task for the provision of data lineage. As the data flow in a virtualized environment within the Cloud is no longer linear, it complicates the task of mapping the data flow to provide data integrity. Managing data integrity is a critical issue in the Cloud, because of the shared environment. Data-at-rest refers to data that is kept in cloud storage that requires the policies of the logical, physical, and access control.

The major issue in data-at-rest in the cloud is losing control due to the data accessing by unauthorized users in a shared environment. In-built encryption schemes in storage are not able to avert unauthorized access as an attacker can steal keys used for encryption/decryption. A lockbox method in which the real keys are kept in a lockbox and there is another key for the lockbox that can be used for the mentioned scenario but with the requirement of lockbox key, it can cause key management the issue. Data remanence refers to data which is left out after transfer or removal of VM. Data recovery is preferred when data is lost because of some accidental damage. Data segregation is the organization of the data of various users residing in the same location. Ensuring the isolation between the user's data is an important security concern. Data integrity ensures that there is no illegitimate modification in the user's data [101]. Data deduplication is an approach for removing duplicate copies of data. Secure data deduplication is a major research concern [102]. Data recovery is another biggest challenging issue. There is the possibility for natural tragedy or accidental harm to the storage devices and due to these reasons, data can be destroyed and data availability can be at risk. Data location, finding the data location is critical in the cloud environment, as data of the user are placed dynamically from one country to another. This raises security and data privacy risk as the data possessor can lose control of his data. In data moving or data removing, data left out, known as data Remanence. Due to it, there is less security threat such as the expose of critical information.

3.3.5 Identity management and access control

Identity management and access control issues are also important security concern. Identity management (IDM) deals with identifying the entities in cloud and controlling their access to resources. Information privacy and sensitivity are highly dependent on the IDM policies and mechanisms in cloud. Identity authentication and verifying them are the features of identity

management. So, avoiding information accessing from unauthorized access is a big concern in the cloud. Identify management is a wide administrative area that has the responsibilities to recognize the individual entities, cloud entity, managing resource access as per predefined policies [103].

As the customers' credentials are transmitted via internet, it imposes a great risk to user's sensitive data. The issue is addressed by providing the support for federation protocols such as Service Provisioning Markup Language (SPML) or Security Assertion Markup Language (SAML) [104] to some extent. SAML supports both authentication and authorization. Some other protocols are created after SAML such as OpenID and OAuth2. OAuth2 is an open standard for authorization and OpenID is an open standard for authentication. The cloud-based IDM are prone to serious threats such as brute-force attack, cookie replay attacks, eavesdropping attack, denial of service attack and data tampering attack, etc. There is a need to design strong security measures for IDM systems. There is a need of providing fine-grained access control mechanisms for controlling access to user's data. For example, Google App uses eXtensible Access Control Markup Language (XACML) for authorization and access control. Mon et al. [105] combined the Attribute-based Access Control with Role-based Access Control (RBAC) to ensure the privacy and security of user's data.

3.3.6 Improper cryptographic keys management

Improper cryptographic keys management leads to failure of cloud security measures [106]. The cryptographic approaches such as cryptographic hash function, digital signature and message authentication code, etc. are used to authenticate the VM templates in cloud. They may prone to the bootstrapping problem and hence, requires a strong security analysis. The key security requirements for key management systems must be ensured. Some of them are discussed as follows. The key management commands and data should be secure from spoofing and illegitimate modification. The third party who does key management should be authentic. All the secret and private keys should also be protected from disclosure. The cryptographic mechanism employed for protecting keys should be strong enough and robust from attacks.

There are a variety of security algorithms that can be used to confirm data privacy and confidentiality from service providers. An encryption approach provides adequately robust security. ABE (Attribute-based Encryption) is a recently designed public key cryptographic approach that works in a one-to-many manner, also known as fuzzy encryption. Public key encryption approaches save encrypted data on third-party servers and decryption keys are distributed to authorized clients. Though, there are various limitations in it, such as this is hard the private keys distribution efficiently to the valid customers, scalability and flexibility problem and It is necessary for data possessors to be online when data is encrypted or re-encrypted data, or private keys are distributed. The Attribute-based Encryption approach reduces

the mentioned confines by minimizing the internet overhead of communication and growing scalability, and fine-grained access control and flexibility for huge-scale systems.

3.3.7 Service level agreement (SLA)

Service level agreement (SLA) and trust level security is another important concern. The customers lose their control over data and programs which are outsourced to cloud servers. Cloud service providers limit the visibility of data location, network and system monitoring to customers which generate the trust issues with service provider. It is very difficult to assure trust in cloud environment. However, the use of signature techniques and advanced cryptographic techniques can be used to deal with the trust issues to some extent. SLA is another way to deal with the trust issues to certain limit. An SLA is signed at the time of registration, describing the minimum performance criteria a CSP should meet when delivering services. If a certain service fails to meet the customers need or quality of service (QoS) do not meet the SLA, cloud customers can lose their trust with the CSP [64].

The clients do not have total control over the cloud resources, but they must ensure the availability, reliability, and resource quality offered by cloud service providers after cloud migration, which is possible with a service level agreement (SLA). With SLA, the clients can use cloud services securely, hence it needs reputation administration. SLA comprises performance, coarseness, clarity vs. complexity, and tradeoffs to fend client requirements and expectations. The cutting-edge SLA schemes rely on clients' feedback concerning main issues such as Cloud interoperability and what is to be migrated. There are various kinds of resources for cloud migration, such as applications related to business, IT organization, deployment of the application. There are various issues that are required to be addressed when business data is migrated. The other challenge is interoperability, in which many clouds that have different methods of client communications with the cloud. Interoperability purposes of identifying the smooth data flow across cloud.

3.3.8 Regular audit and compliances

Regular audit and compliances to manage cloud resources must be done to ensure whether internal and external processes are meeting the customer requirements, regulations and laws. The policies should be monitored regularly. There are some general governance standards that are also applicable to cloud computing environment such as ISO/IEC 38500 – IT Governance [107], Control Objectives for Information and Related Technology (COBIT) [108], Cloud Security Alliance (CSA) Cloud Controls Matrix [109], etc. The law and regulations of different countries are different. Therefore, some of the compliance operate at country-level, or regional-level [64]. Some of the standards are applicable to specific company or data. The Health Insurance Portability

and Accountability Act (HIPAA) [110] requires the U.S. health care organization to maintain the confidentiality of protected health information (PHI). Payment Card Industry Data Security Standard (PCI-DSS) [111] defines the minimum security controls to secure the customer data. The Federal Information Security Modernization Act (FISMA) [112] is a compliance framework that enforces the protection of information systems and assets of all federal government agencies and contractors. Sarbanes-Oxley Act (SOX) [113], a federal regulation, provides the standards for all U.S. publicly traded companies to ensure security to all shareholders and public from fraudulent actions. It maintains the information policies and prevent the illegitimate data tampering.

3.3.9 Cloud and CSP migration, SLA and trust level issues

One of the major issues in the cloud environment is trust level issues. As cloud customers have control deficiency on resources, they have to depend on trust schemes agreements in alliance with schemes that offer compensation. In a heterogeneous environment, trust calculation is complex which is measured by a social trust or human. Services may be sub-serving without awareness of the customers. The customers have less visibility of system monitoring and networks that is a big trust challenge. The staff who have authorized access and can be malicious insiders in the organization and attacks could be executed that can influence the privacy and confidentiality of other customer's data and also resources. There can be a trust problem due to public relations lacking. Trust problems can be addressed by offering suitable measures for the visibility of the observing system. There must be means for dealing with the related risks. Access control vulnerability, Cross-site scripting, doubtful configuration, and storage are few examples of threats.

Service Level Agreements (SLA) is an agreement between the service providers and their clients that documents the services provided by the providers and states the service standards. Most SLAs attention to contracts concerning the attempt that will be performed by Software-intensive systems (SIS) providers when the problem takes place. Though, no assurances are stated concerning the service's efficiency for business processes of the client and their business purposes. The issue of availability, unintended resource allocation, deceptive computation, and loss of data are, however, issues that can tamper SLAs [114]. Cloud and CSP Migration, when the users migrate to the cloud, they move their complete setup to the cloud. Where the provider will maintain the computing environment. Though, that is a difficult procedure for several organizations since they had to leave off a specific level of control to the cloud provider. Also, the transfer in itself is a challenge since there are certain aspects in it that the user has to be attentive. When an organization or cloud customer is entering into the cloud or shifting from one CSP to another CSP, the following migrations will be considered: Data (application) migration and Cloud migration. Migration is one of the challenging research areas.

It involves the secure transmission of the tenants' data with strong application and network security measures together with governance compliance. There are many questions that need to be resolved with tenants such as What technology is used in migration? Is the CSP migrating the data with appropriate policies in place? Is the migrated data secure? Is the migration secure from attackers? etc [115].

3.3.10 Hardware-level security issues

The hardware layer is the lowest level in the stack. The hardware or physical level is employed in data centers. At the hardware level, all hardware resources such as physical servers, switches, routers, cooling, and power system are maintained. The hardware layer can also be termed as the physical or server layer. The applications are used by the service providers to observe memory, CPU loads, storage, etc. The users can interact only with the virtualized environment. The adversaries can exploit the hardware layer and can gain physical access to the system. They break the security at the hardware layer and perform attacks on the data integrity and privacy that exist on the secondary storage and main memory. Trusted Platform Module (TPM) may be altered to dump the data of the internal registers and sensitive data can be fetched like the secret key. The adversary obtains a message that is exchanged between TPM and authorized user and after that message can be misused maliciously. Attacks such as side-channel can be performed. The access to the physical resources such as network devices, storage, and processing servers must be constrained physically only authorized persons must be allowed with security authorization to manage the actions. Some hardware-based solutions [116] for cloud focus more on hardware security.

Researchers are working in different domains of security as discussed above to address the security issues. We have considered intrusion detection as one of the key security aspects to detect attacks at different layers in cloud. The security issues are briefly described in Table 3.1.

3.4 Security Requirements for Privacy

Privacy is a more critical issue than security due to dealing with the public. The cloud service provider has the opportunity to examine and escapade large volume of personal data one example is, the service provider could know the number of persons who are suffering from cancer due to showing their interest to search chemotherapy which could be shared to the organization related to the insurance that could use this information to categorize a person as higher-risk for greater premium. We discuss some security requirements below:

TABLE 3.1: Security issues

Security Issues	Sub Category	Threat/Vulnerabilities	Solution
Virtualization level security Issues [117, 101, 91] [118, 119] [91] [120] [91]	Monitoring virtual machines	Untrusted hypervisor element, hypervisor-based rootkits, Hypervisor inspection, isolation, interposition, zero-day attacks, VM escape	Better authentication and authorization. Strong isolation between VMs. Use of secure hypervisor. Monitor activities at the hypervisor.
	VM-level	Side-channel attacks, VM hopping, cross-VM attacks, Malware injection, Covert-channel attacks, VM reset vulnerabilities	
	Virtualized networking	Packet sniffing and spoofing, Impact of network security devices on virtual networks, Virtualized communication channels	
	Managing images	VM sprawl, Image stealing and code injection, Large-sized images cryptographic overhead	
	Mobility	Live VM migration MITM attack, VM mobility, VM cloning	
	Malware	VM rollback, Malware escape approaches, Malware expanding to the VMs	
[67] Service Level Agreement	Cost	Service price associated issues,	Cost management based on SLA overcomes these problems and gives an effective solution for controlling the cost of allocated resources based on the hosted application's defined policies.
	Resources	Not giving the particularized quantity of resources,	
	Risk management	Risk computation management to control the resources allocation based on SLA	

TABLE 3.1: Security issues

Security Issues	Sub Category	Threat/Vulnerabilities	Solution
	Waiting time	Customers waiting in line for an extended duration for using service	
	Performance	Service Performance may be affected due to the high workload. The clients will not be fulfilled due to bad performance and the revenue will be affected	
	SLA negotiation	Applications must perform in the care of their consumers and cloud services must be available in SLA negotiation.	
Cloud and CSP Migration, and Trust level issues [121]	Service provider, cloud migration and Trust	Cross-site scripting, access control weaknesses, insecure storage, and insecure configuration	Advanced cryptographic techniques and signature techniques
Application Level Security Issues [64, 122]	Unauthorized Accessing	SQL Injection attack, EDoS, Cross-site scripting, Cookie Poisoning, Google Hacking, Hidden field manipulation, Backdoor and debug options	Check service integrity using a hash function. Web service security. Use secure web browsers and APIs.
Data security	Data Integrity, Confidentiality and Access	The adversary in the network affects the confidentiality and the integrity of data, non-authorized user accesses	lockbox approach

TABLE 3.1: Security issues

Security Issues	Sub Category	Threat/Vulnerabilities	Solution
Identity management [123] and access control	Identity and access control	Signature Wrapping Attack	Data should be transmitted via a secured channel and fine-grained. Authentication and authorization techniques, hierarchical identity-based cryptography (HIBC)
Network Level Security Issues [64, 122]	Data confidentiality	Eavesdropping, Port Scanning, Replay attack, Sybil attack, Reused IP address, DDoS attack, BGP Prefix Hijacking, DNS Attacks, Sniffer Attack, DoS attack	IPsec Implement security policies. Clearance of Old ARP addresses from the cache. Proper configuration, MD5/TTL protection Restriction of ICMP and SYN packets on the router interfaces. Domain name system security Extensions
	Data availability		
	Data Integrity		

3.4.1 Fine-grained access control

Fine-grained access control commonly used method in the cloud environment. Using this mechanism every data entity is assigned its own access control policy. Every user can access only its data for which he is allowed and he should not be able to access data for which he is unauthorized. One who wants to access the data entity requires to provide its authorizations to a policy enforcer (not data owner in the cloud). For example, when an organization keeps data in the cloud, the organization allows only some authorized persons who are related to the projects, can see the data. The access control policies and the authorizations may disclose some information that is not allowed for the policy enforcer. To control the access to susceptible data or code fine-grained access controls must be accessible. In cloud computing, Cryptography is a good option to attain fine-grained access control [124]. In these schemes, Attribute-Based Encryption (ABE) is applied for data encryption. The decryption only can be performed by those who have the required attributes. These types of access control schemes are created by the storage service provider to store the data. To cloud resources control accessing, eXtensible Access Control Markup Language (XACML) standard is used for access policies. Some examples using XACML are GoogleMaps and salesforce, these providers use it for access control and authorization selection. The one challenge with the fine-grained access control methods is the policy enforcers can see partially the access control policies.

3.4.2 Privacy-preserving

Cloud computing is very powerful as compared to personal computing but the cloud also comes with new security issues to the data of the users. Data security and user privacy meet with various threats. Lots of work have been done to preserve the privacy of the user. The privacy information of users such as user credentials should not be revealed to the cloud. To understand the powerful and privacy-preserving service of data sharing in the cloud environment, some requirements must be attained such as the data possessor must be able o take decide that who can access his data in the cloud. Another is, the user's privacy must be secured in the cloud and lastly, the data must be accessed by low computing devices such as tablets and smartphones, etc. Dynamic accumulator-based technique for privacy-preserving access control has proposed by Slamanig [79], in which permissions read, delete, write are given by using Access Control List (ACL) to other users who can do tasks on outsourced data elements with mentioned permissions. With this technique granting or denying access can be decided. The user of the data can allow or gain access permissions to/from other users, although the Cloud service provider cannot recognize these users. The drawback of this technique is that if the owner of the data wishes to repeal permission from the user, then that user has to repeal given permissions from other users. This is complex computation to manage the chain of users.

3.4.3 Collision resistance

No user should not be allowed to share her/his private key user. Users cannot decrypt encrypted data by merging their features because each feature is associated with a random number or polynomial. Merging features from several sets of features within a specified key is an actual issue. Avoiding collision by ignoring users

from merging features from several keys is another issue. Park et al. [125] presented Sec-DPoS a deduplicatable proof of storage system which is based on the symmetric key that guarantees confidentiality with brute-force attack resilience. It supports symmetric key cryptography-based integrity auditing of the outsourced data. They described some building blocks such as collision-resistant hash function, pseudorandom function, key derivation function, and pseudorandom permutation, authenticated encryption, deterministic symmetric encryption.

They have four protocols in their system. Key and index distribution protocol, initial upload protocol, and the Deduplication Protocol , and finally they discuss the integrity auditing protocol. In key and index distribution protocol, a preliminary uploader creates a possible response set for a file to audit Integrity with the help of a message-derived key that is distributed from the management server. The file and possible response set is uploaded. The other customer who is using the same file then he can use the possible response set created by the previous uploader. In the initial upload protocol, it is considered that the uploaded file is new data not earlier uploaded. Therefore, the customer creates the possible response set which will be used in the integrity auditing and another possible response set is created by the cloud server that will be used for ownership check. In the deduplication protocol, the deduplication procedure considers that the uploaded file is a duplicated data from an earlier upload. Therefore, the cloud server must check that the customer has the file. And in integrity auditing protocol, the customer who is the file owner then he can audit outsourced data's integrity at any time.

3.5 Privacy Issues in Cloud

Cloud computing uses virtualization technology, so, the personal information of the users may be dispersed in several virtualized data centers. When users access cloud services, they may disclose private information. The major goal of cloud security is securing data privacy. It is hard to avoid threats in a cloud environment due to its sharing environment that relies on a shared infrastructure. Therefore, data will be unprotected from unauthorized access. There are some privacy-related issues are discussed below.

3.5.1 Defining roles to actors

In the cloud environment, there are many types of the actor with different privilege. The main actor is the owner of the data, which can be called the data owner. Another important factor is the cloud service provider who can process private data like transfer, storage, research duplicate, etc and able to perform undeclared activities that can be a threat to data privacy like they can reveal private data by reading and also they could obtain user's data that can be useful for big financial advantage. Cloud-based services actors that may require to access private information to perform some actions and is the owner of the service who have the access to the database from where he can access the private information of the users [126].

Some other actors are cloud auditor, cloud agent, and cloud carrier. The cloud carrier is a mediator that makes available connectivity and transportation of cloud services from Cloud service providers to cloud Customers. The cloud broker is the individual who controls the routine, performance, and provision of cloud services and negotiates associations between service providers and cloud customers. The cloud auditor is the entity that can perform an independent evaluation of cloud services, performance, information system operations, and cloud security employment.

3.5.2 Compliance

Compliance states the responsibility of the company to work in agreement with existing standards, rules, and regulations. Different countries have their security and privacy rules and regulations that make compliance very complex and it becomes a critical issue in the cloud. Data location is a big challenge for the organization in compliance. The Service Level Agreement is important in the cloud base system. This is the agreement that is signed by the communicating parties that contain rule and regulation and all service information. There are various compliance issues, such as data sites or laws and regulations. Data site is the general compliance challenge encountered by the companies [127]. The organizations that use an internal computing center permit to design their computing environment.

Hence they have the detail information about the data storage and what security is being used, whereas, in various cloud computing services, data are warehoused in many physical sites, and complete information about the site of the data of the companies is not available or not open for the service users. This condition makes it problematic to determine whether adequate protections are in location and whether legal and governing compliance needs are met, such as NARA regulations that have ability requirements federal records storage and instruct the least height above and move away from a flood plain. The other issue is law and regulations, for U.S. Federal agencies, the key privacy and security compliance involves the Office of Management and Budget (OMB), Clinger-Cohen Act of 1996, 1974 privacy Act, 2002 E-Government Act like FISMA .

3.5.3 Legal issues and multi-location issues

The cloud business model adopts Service Level Agreement to specify the contracts over a particular service. This service might be SaaS, PaaS, or IaaS. The Service Level Agreement is contracted to legally decide the cost per service. Therefore, there can be an indirect subjectivity on the attainment of these contracts. The cloud actions increase several legal and challenges. The most important is the multi-location specific properties in cloud computing. Cloud service providers have the data centers in which they have sufficient resources to be spread worldwide. Irrespective of that, few countries do not permit data to leave their borders. Due to this situation, many challenges arise. If data moves beyond the boundaries, it is difficult to know due to which country jurisdiction data crashes. If it happens, it is difficult to declare to which area legal jurisdiction can reach to discover liable parties. It contains evaluating that government departments are able to access the data outside the boundaries of the country in which information was created in the first place.

3.5.4 Privacy issues on CIA

Privacy of the data has issues on integrity, authorized access, or availability. When information is copied or stolen by an unauthorized user , this condition is known as a confidentiality loss. When information is changed in an unexpected means, this condition is known as integrity loss. When information is missing or not accessible, this condition is known as availability loss. The data integrity provides the surety that data has not been modified during communication. Authorized access avoids data from attacks whereas backups and copies permit access of data properly even technical issues. Data is communicated at the common network backbone. Therefore, attackers can position concealed proxy applications between the Cloud service provider and customer to look for session detail and login credentials information of login. Attackers may do IP-spoofing or packet sniffing and they can get access to sensitive information.

Cloud services must be available all the time. In Infrastructure-as-a-service, the availability of hardware and logical resources such as computing servers and databases are required to run processing operations of programs and operations related to obtaining the data, respectively. Subashini et al. [101] discussed that a multi-tier design must be embraced that is reinforced by a load-balanced farm of application instances operating on various servers. This method lets DoS attacks resiliency by developing software and hardware breakdown measures in every tier.

3.5.5 Protection of the data

In the public cloud, the gathered data exists in the shared environment. Organizations keep sensitive data in the public cloud. There is a requirement of mechanisms in place so that the data access can be controlled and the data is stored securely. In today's era, data is currency and cloud storage is bank safe. Data is becoming gradually favorite target because of collective values [128]. The companies that have gathered data is at high risk and may cause DoS, as an accidental loss from an attack targeted against the companies. The physical attacks against the cloud resources of prestigious companies have side effects. For data security, data sanitization and isolation of data approaches can be used. Data can be found in various forms such as application development in the cloud and data can be scripts, programs, etc.

For installed applications, it contains records and other data produced or used by the applications. The access control methods are one way to keep data away from unauthorized clients. Furthermore, the method is encryption. Access control can be client's identity-based authentication that is a critical challenge in the cloud. Encryption is the only method to ensure the security of the data as less physical control over data storage. The data sanitization performs that a cloud service provider implements have apparent security effects. Sanitization contains erasing data from storage by overwriting or demagnetizing, or destroying media itself to avoid unauthorized exposure of data.

3.5.6 User control lacking

The private data are warehoused in the public cloud in distant machines that are controlled by the cloud service provider. There is a need for transparency for storage location, copies of data, and data processing. Sometimes it is almost impossible to

get to know about privacy violations and who did them. In the cloud computing environment, computation and customer's sensitive data sharing do not have sufficient control, heading to threats such as stolen, exploit, or unauthorized access [129]. The software-as-a-service platform provides control of the data to the service provider, so the data control and visibility will be restricted. The attacker can steal or corrupt the data as users do not have control over the cloud. Moreover, there is no data transparency, for instance, data location, ownership of data, and data usage. Though data disclosure can occur during data moving, various countries have the law for data accessing if they suspect. A user control can be either a legal problem or one raised by the user himself.

3.5.7 Data movement

Data movement can occur between countries and local rules. Hence, it is another big challenge in the cloud environment. Data invisibility can be the solution for the privacy and security of the data of users. Fatema et al. [130] presented a . This model provides visibility into the place of data. XML-based policies are used in this model. The one drawback is a single point of failure. The central controller is inside the cloud and manages all data accesses and also data movement. If the accesses are made inside the same cloud, it can be the bottleneck. They consider inter-cloud data transfer, but every cloud needs to be managed own policy archive. The Directive of the European Union to secure the data (95/46/EC) related to moving personal data to the third countries came into existence in 1998 that permits moving sensitive data to third countries. The regulation and directives of the European Union are used to tie its member states. As an outcome, the United States Department of Commerce proposed a contract to permit the United States-based organization to share private data with their European complements without disruptions.

Some other privacy issues such as resource privacy sharing, sharing resource privacy in the cloud environment with protecting users is a significant issue. Data isolation can be used as a solution to this issue in which isolation is provided for each user's data, and one more big privacy issue is the data source nature as data comes from various sources. So, it is necessary to secure and control the data carefully, and only authorized users can access the data. Privacy of users must be controlled when data is gathered, warehoused, or carried. Data gathering from various sources is challenging in cloud computing because it exposes sensitive information of the users. To attain an adequate level of privacy in cloud, various problems need to be discussed, such as inadequate customer control over their data, data revealing in-transit across the cloud, illegal secondary storage of delicate data, uncontrolled data propagation, and dynamic provision of legal difficulties [131]. One other issue is the advanced service level agreement method relies on the customers' feedback concerning significant challenges such as Cloud interoperability, data, resources, and processes that can be moved to the cloud.

3.6 Conclusion

Cloud computing has evolved over the years. Security is one of the primary concerns in cloud environment. In this chapter, various definitions of security and privacy are provided first. Furthermore, various cloud security goals are discussed. Various issues related to cloud security are explained in detail with viable solutions. In addition, security requirements for the privacy are explained to give reader deep understanding on privacy aspects in cloud. Furthermore, an various privacy issues are discussed. We hope that this chapter will give a good knowledge about the security and privacy concepts in cloud.

3.7 Questions

Fill in the blanks

1. Mark the correct privacy issues in cloud

   i Protection of data
   ii Lacking of user control
   iii Data movement across countries
   iv All of above

2. Data linage refers to trace the path of the data and this is essential for auditing in the cloud.

   i Trace the path of the data and this is essential for auditing in the cloud.
   ii Unauthorized use of data in a shared environment
   iii Unwanted modifications in the data
   iv Unrestricted access to data

3. The unavailability of services is the

   i Network level security issue
   ii Application level security issue
   iii Data security level issue
   iv Virtualization level security issue

4. Access control features can be used

   i To maintain the control on access to the resources.
   ii To know what is going on in cloud
   iii To enable the remote data access
   iv None of the above

5. Mark the incorrect statement

   i Data integrity is the basic task that verifies the data and it provides the guarantee for the exactness and quality of the data.
   ii The goal of availability is to provide the services to its users without modification.
   iii Authentication is the method of creating assurance in the identities of the user.
   iv Auditing is the monitoring task to know what is going on in the cloud-based system.

Short-Answer Questions

1. Describe application-level security issues.
2. Why privacy is a research challenge in cloud? What are the security requirements of privacy.
3. What is the difference between confidentiality, integrity and availability?

Long-Answer Questions

1. Define privacy. What are key privacy issues in cloud?
2. Describe virtualization-level security issues and data security issues in cloud.

Part II

Threat Model, Attacks, Defense Systems, and Security Techniques