iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6362

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Cloud Computing and Privacy Risks in the Information/Knowledge/Digital Risk Society and Economy: An Overview

Sompurna Bhadra
PhD scholar, Department of Computer Science and Engineering, Techno India University, Kolkata, West Bengal- 700091

Abstract: ***Cloud computing has revolutionised the way in which computing services are delivered and managed in the contemporary society and economy. The emergence of computers and the internet, the one hand, accelerated the swift technological developments in especially in the computing domain thus speeding up the rapid growth and diffusion of cloud computing. But, at one and the same time, on the other hand, they tectonically transformed the contemporary society and economy into information/knowledge/ digital society and economy. Both are reciprocally and interactively related, strengthening each other in their operational and functional practices. These practices, in the wake of coming of 'data revolution' and consequent 'datafication' of the society and economy, abundantly exhibited different types of security issues, especially privacy risks, which transmuted the erstwhile society and economy into an the information/knowledge/ digital risk society and economy and, simultaneously, became an hindrance to the diffusion of cloud computing, which itself is embedded in this risk society and economy in the global information capitalist order. Risks, particularly privacy risks, constitute the strong bridge and link between them. The present paper critically analyses and surveys these stated socio-technical developments.***
Keywords: Cloud Computing, Computer, Internet, Privacy Risks, Information Risk Society and Economy

I. INTRODUCTION

The impact of the Information and Communication Technologies (hereafter ICTs) in revamping structural transformation is enormous and multifarious. It is more transformative and empowering when one takes account of the ecosystem of the ICTs, which comprises other newly emerged innovative technologies such as IoT, Big Data, Data Analytics, Cloud Computing, etc. ITU (International Telecommunication Union) refers to the emerging ICT ecosystem, providing different types of benefits. The following Figure 1, provided by ITU, illustrates the Information and Communication Technology ecosystem and its components



Figure 1: Complementary Innovations in Advanced ICTs

[1]. IoT, Cloud computing, big data analytics and artificial intelligence each has useful applications on a standalone basis. But, if they are technologically jointly used, the combination will provide greater benefits. This is so in view of the increased capability of each technology when used in unison along with next-generation networks (NGN) and new applications or services. As ITUstates:

©IJRASET: All Rights are Reserved

'IoT can unfold its true potential when combined with data analytical capability. Given the rapidly increasing amounts of information, their velocity and complexity, artificial intelligence can greatly help to make sense of the information and create semi-autonomous and autonomous cyber–physical systems (such as autonomous vehicles, smart homes, smart grids and smart transportation). Sensors, actuators and networks form the physical backbone of IoT in a narrow sense. Cloud and other new computing architectures provide a complementary layer of data processing and storage capabilities that enables ubiquitously available services. Big data analysis helps to make descriptive, explanatory, predictive and prescriptive sense of the detailed data. Artificial intelligence enhances all these capabilities (e.g. computer vision allows new forms of sensing) but also, most importantly, adds another layer of analytical power. Most of the value in this new technology stack is in the applications and services that can be created by using IoT, cloud computing, big data analytics and artificial intelligence ... in a wide range of verticals (e.g. energy, transportation and health care) and across sectors' [1]. In addition ICTs, cloud computing as core technology, together with other technologies (i.e., IOT, Big Data Analytics etc), contributes to attaining sustainable development Goals(SDGs) across the world. Table 1, taken from ITU's *Measuring the Information Society Report* (2017), show how ICTs are advance these goals [1]. They all are constituents of the Fourth IndustrialRevolution [2], as shown in Figure 2. From the Fourth Industrial Revolution emanated the concepts such as Internet of things (IoT), industrial Internet of things (IIoT), cobot (collaborative robot), big data, cloud computing, virtual manufacturing, and 3D printing, artificial intelligence, biotechnology and others [3]. The Fourth Industrial Revolution is integrally specifically connected with such disciplinary areas, argue Kumar and others, "as intelligent manufacturing, cloud manufacturing and Industry 4.0 and key enabling technologies such as big data analytics, cyber-physical systems, Internet of things, information and communication technology and cloud computing" [4] How (CC) is connected to Robotics, which emerged during the Fourth Industrial Revolution is connected is shown, for example, by a recent researcher: 'CR is a rapidly evolving field that allows robots to offload computation-intensive and storage-intensive jobs into the cloud. Robots are limited in terms of computational capacity, memory and storage. Cloud provides unlimited computation power, memory, storage and especially collaboration opportunity' [5]. In brief, 'Cloud computing combines the best of the mainframe era with the best of the PC-enabled client-server era along with the Internet era' [6]. Far from being a hype or catchphrase, Cloud Computing (hereafter CC) is an emerging paradigm and a transformational technology that renders numerous services to a host of entities ranging from individuals and businesses, through various governmental and on-governmental organizations and agencies, to IT professionals including academics and researchers by virtualized centralization of computing shared resources over the internet from any location (home, workplace etc.). To the client CC offers serviceslike applications, data, computing resources and even management functions. 'Individuals are using cloud-based applications, such as Web mail and Web-based calendar or photo-sharing Web sites (e.g., Flickr, Picasa) and online data storage. Small- and medium-sized enterprises are using cloud-based applications for accounting, payroll processing, customer relationship management (CRM), business intelligence, and data mining. Large enterprises use cloud services for business functions, such as supply-chain management, data storage, big data analytics, business process management, CRM, modeling and simulation, and application development'[7]. Sosinky makes the point that the word 'cloud' has specific reference to two essential concepts in CC. The first one is abstraction in the sense that it abstracts the details of system implementation from both users and developers. This implies that 'applications run on physical systems that aren't specified, data is stored in locations that are unknown, administration of systems is outsourced to others, and access by users is Ubiquitous'. The second essential point is that CC 'virtualizes systems by pooling and sharing resources. Systems and storage can be provisioned as needed from a centralized infrastructure, costs are assessed on a metered basis, multi-tenancy is enabled, and resources are scalable with agility' [8].

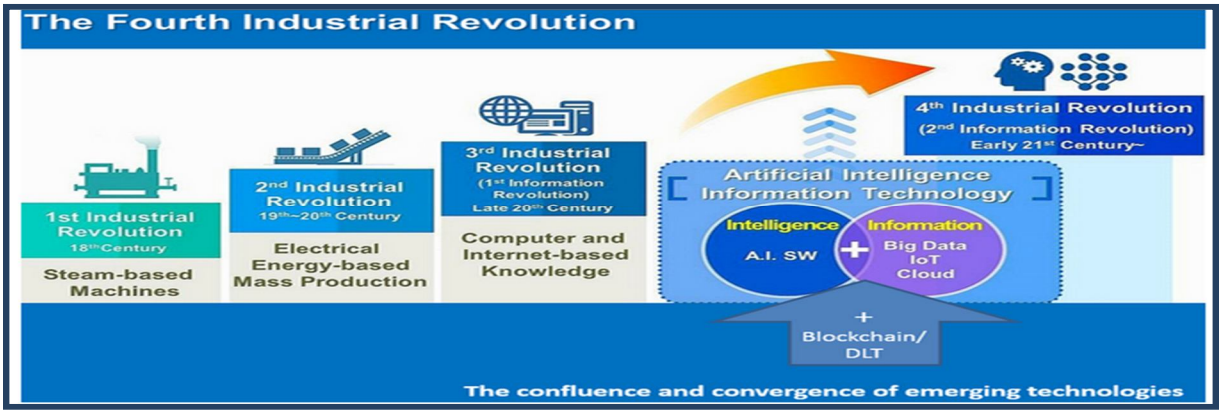


Figure 2: Fourth Industrial Revolution

©IJRASET: All Rights are Reserved

The analysis of the issues raised in the instant paper follows the following order. The section II discusses different dimensions of CC with special reference to its historical background and evolution. In section III the development of the information/knowledge/digital society and economy is mapped out in its multidimensional aspects and components. The section IV shifts the analysis to highlighting security, data security and privacy concerns in CC in the information/Knowledge/ digital Society. Next section V concentrates on privacyand privacy risks of privacy in cloud computing and assesses the role computer and internet in this regard. The final section VI points to the findings of the study showing the parallels between the emergence of theInformation or knowledge or digital society and economy, on the one hand, and CC, on the other, in terms of privacy risks that are embodied in both. Research method applied to this kind of research work is known asexploratory study. Its scope is as follows: "Exploratory studies consist of collecting, analyzing, and interpretingobservations about known designs, systems, or models, or about abstract theories or subjects. These studies are largely an inductive process to gain understanding. ...Exploratory studies observe specific phenomena to look for patterns and arrive at a general theory of behaviour. The emphasis is onevaluation or analysis of data, not on creating new designsor models. The emphasis is on perspective and relativeimportance [253]."

II. HISTORICAL BACKROUND: AN OVERVIEW OF CLOUD COMPUTING

The CC historically evolved in terms of cumulative technological developments that were innovated since the 1960s. It came into prominence in 2006 when 'Amazon launched its Elastic Compute cloud (EC2) as a commercial web service that allows small companies and individuals to rent computers on which to run their own computer applications'[9]. Bohm et al. argue that CC emerged in 2007. In Fig. 3 they also provided a historical timeline of its evolution from 1837 to 2007 [10]. Deshpande and

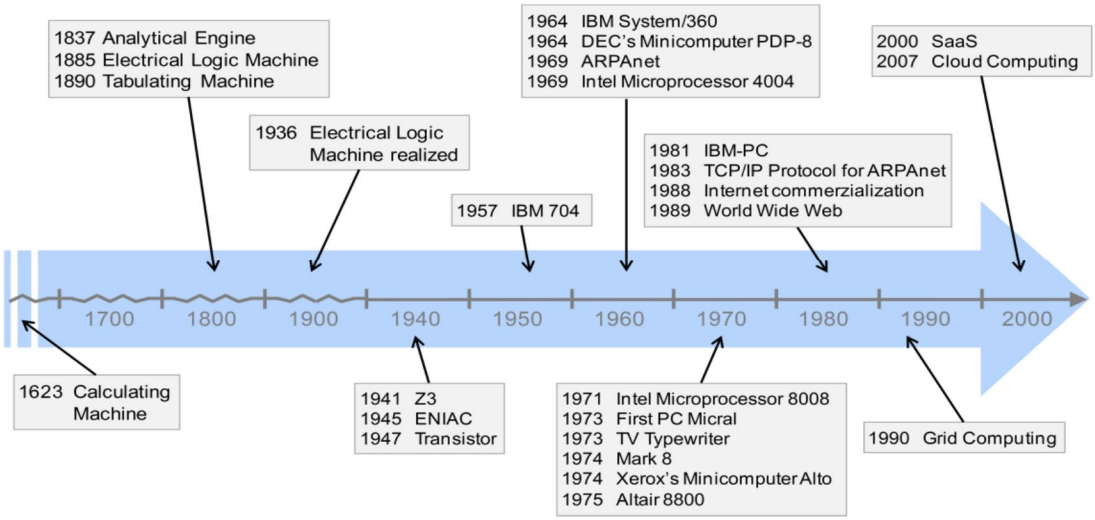


Figure 3: Time of historical milestones of the development of Cloud Computing

Others trace the origins of CC in Terms of their historical relationships to each other. In recent times CC grew outof firstcomputers that evolved from the centralized mainframes (1959) to the distributed client–server regime powered by the dawn of personal computers(1981). Then comes Internet era when one became empowered access from anywhere by means of computer communication network spread across the world. CC emerges, also by being a point of departure for other technologies like, IoT, Big Data and Data Analytics [11]. Figure 3 shows this. It is rightly stated that "Cloud computing is a

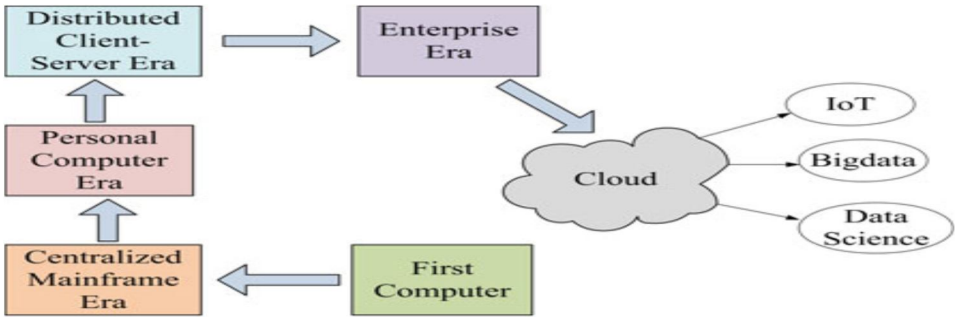


Figure 4: Evolution of Cloud technology

©IJRASET: All Rights are Reserved

Combination of best from mainframes, client–server models and Internet technology" [11]. Said otherwise, historically CC is the product of successive technological advancements, as in Figure 4 which shows the convergence of technologies leading to the rise of CC *per se as in* Figure 5 [12]. What is cloud computing? It is rather difficult to define what CC is because the there is no consensus among concerned experts on its definition. In the computing domain there are disagreements which usually vary on the basis of emphasis the experts put on while defining CC. The word 'cloud' was initially used in telecommunications industry as an abstraction in the network system and then became the symbol of internet – the computer network. This gave rise finally to cloud computing associated with, as Buyya et al contend, 'an Internet-centric way of computing' since the internet plays a basic role in cloud computing [13]. This is reflected in the definition given by Armbrust et al.: "Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use thatterm. The data center hardware and software is what we will call a Cloud" [14]. Buyya et al. define CC as follows: 'A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers' [13]. The widely accepted definition of cloud computing is one given by NIST (The National Institute of Standards and Technology). According to its 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.(October 25, 2011: 2-1)' [15]. Chen and others mention that there are five actors, as listed by NIST, who are involved in the CC process. 1. Cloud consumer–A person or organization that maintains a business relationship with and uses services offered by cloud providers. 2. Cloud provider–A person, organization, or entity responsible for offering various services to cloud consumers. 3. Cloud auditor–A party that can conduct independent assessments of cloud services, information system operations, performance, and security of cloud implementations. 4. Cloud broker–An entity that manages theuse, performance, and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers. 5. Cloud carrier–The intermediary that provides connectivity and transport of cloud servicesfrom cloud providers to cloud consumers [16]. Figure 6 presents an overview of the NIST cloud computing reference architecture, which includes the major actors, their activities and functions in CC [17].

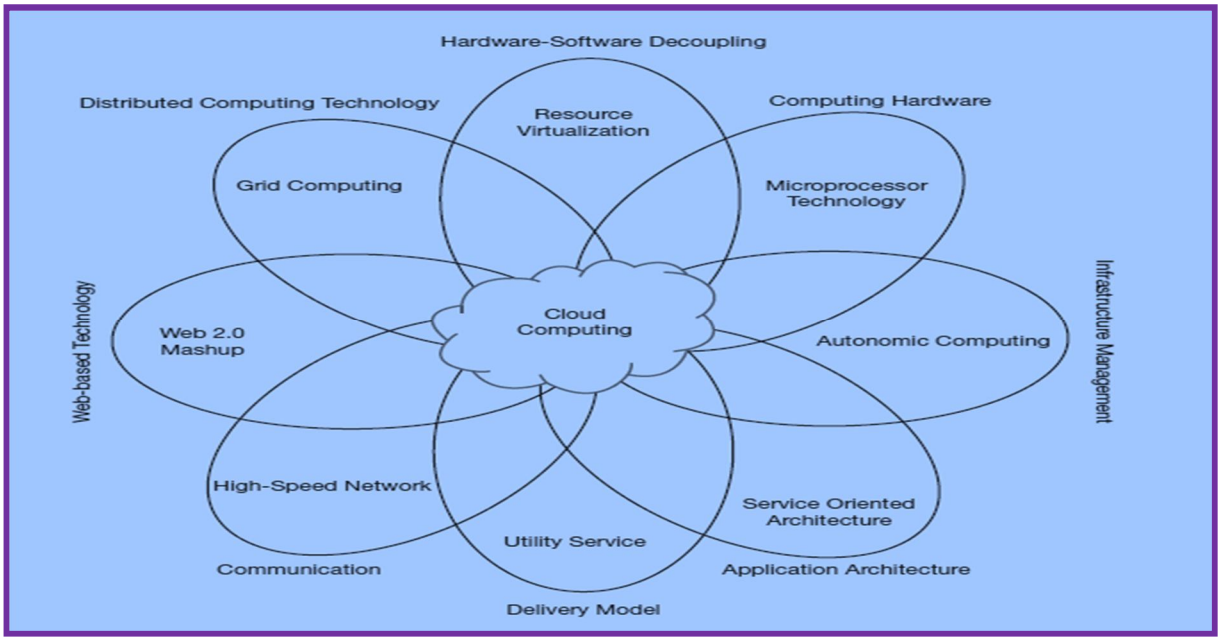


Figure 5: Convergence of technologies for evolution of cloud computing

In this respect, architecturally speaking, CC it consists of a Frontend and a Backend segments. The Frontend refers to the cloud user working on the network (internet) or mobile phone. The frontend is the user interface that the user uses to get connected to the cloud. The user interface enables the user to perform managerial functions such as switching on and switching off virtual machines, overseeing their servers and the various computing resources. The most common application is such that a web browser on which most applications in different devices can be set up because of the added advantage of simplicity and familiarity in its use, as in the

©IJRASET: All Rights are Reserved

World Wide Web (WWW). In today's web browsers, a user can now to run applications via the browser, and thus can access various resources of the cloud via the web [18]. The Backend is concerned with computational devices and processes and data bases. They include various entities, such as the following: 1. Physical machines data centre for managing the physical resources of cloud computing and hence inclusive of servers, switches, routers and the cooling arrangement; 2. Virtual machines for allocating cloud resources on demand to the user. Virtual machines are tasked with virtualization meaning that resources of one physical machine can be allocated and used by several virtual machines; and 3. Software support based on operating system (OS) and application framework, providing the platform for the Application Programming Interface (API) forstorage and less costly web applications [19]. As Chandran and Angepot argue, CC components can further be illustrated in terms of cloud infrastructure, cloud platform and cloud application. Cloud infrastructure is made up of numerous services such as computational resources like virtual machines, data storage and communication services Amazon's EC2. The cloud platform supplies APIs for interaction with the cloud application like Google's App Engine

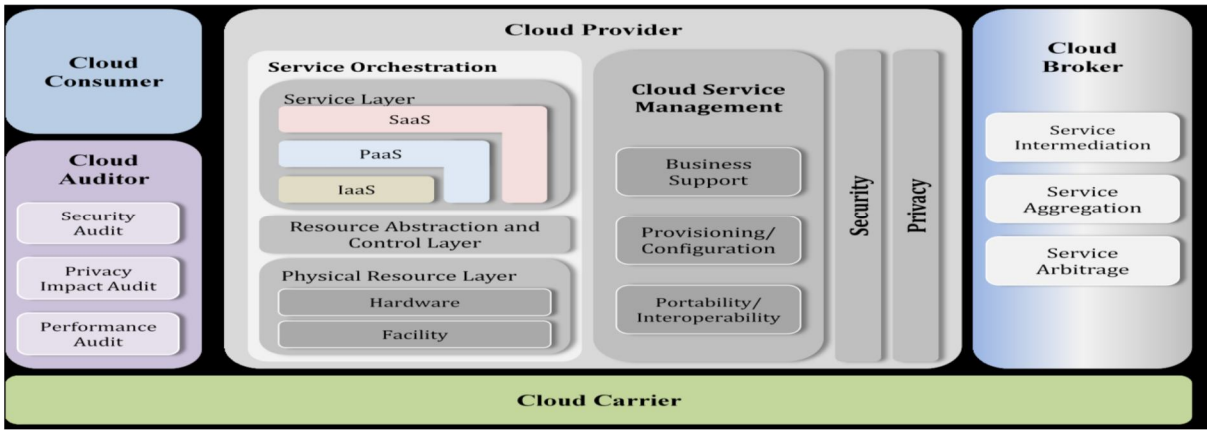


Figure 6: Overview of the NIST cloud computing reference architecture

or Salesforce.com. Finally, cloud application is the web service which runs on the topof the cloud platform or the infrastructure. They are the common interface applications such as the Google's Google docs [20].T he CC exhibits many features which are shown in Figure 7, taken from DataFlair Team [21]. CC offers many gains to the business organizations for which it is adopted as a strategy for commercial benefits in the competitive market. First, CC ensures **Cost Reduction** in capital expenses because business organizations will not have to pay for server hardware since cloud service providers provide in-house provision of



Figure 7: Ten Major Features of Cloud Computing

Computing services. In addition, they only pay for CC services they use. It means that underutilization of services will understandably restricted to the minimum. Second, CC demonstrates improved Flexibilitysince business employees can get CC services from anywhere as long they have access to the internet connectivity through any kind of device. It is therefore location independent. Third, CC has Agility meaning that it can speedily develop, test and launch software applications to respond to thecustomer's requirements andhence can adapt to the changing needs of the business environment. Fourth, CC has Scalabilityin thesystem referring to the ability to promptly increase or decrease the workload (i.e. processing, storage etc.). Thus the scalability enables availability of resources on demand and removable those when not needed. Fifth, CC displays Reliability in that if one physical machine fails, the other physical machines can handle load or tasks dynamically.

©IJRASET: All Rights are Reserved

The failure of the concerned machine remains invisible to the consumers. Sixth, CC thus stands for Reduced Management Efforts because dynamic nature of the CC to flexibly handle hardware failures spares of the need for humanintervention. Seventh, the utilization of CC results in Reduced Environmental Effect because its operations reduce carbon footprint, while assuring better uses of hardware resources with flexibility.Finally, CC ensures Better hardware Resources Utilization, for one host server with higher capacity can replace several other servers as virtual machines [22] [23] [7]. In the following Table 1 Srinivasan summarizes the benefits that accrueto different types of business organizations for using CC [24]. Bhowmik [12] provides a comprehensive list of advantages for using the CC in Figure 7. Even though CC provides substantial benefits to the individual and business consumers, there are several factors which must be considered when they consider its implementation of the CC. Amron et al. [20] have reviewed these factors on the basis of existing literature and mention different factors in Table 2.They also, however, motioned that there are factors that act as inhibitors in the process of implementation of CC, such as (1) security, privacy and trust; (2) compliance; (3) reliability and (5) complexity and interoperability; and (6) vendor lock-in [25].

Business benefits	Small Business	Medium Sized Business	Large Business
Service availability	Y	Y	Y
Service reliability	Y	Y	Y
Meeting demand elasticity	Y	Y	Y
Ability to pay -as you-go	Y	Y	Y
Service automation	-	Y	Y
Email support	Y	Y	-
Database support	Y	Y	-
CRM support	-	Y	Y
Access control support	-	-	Y
Security	-	-	Y
Business continuity	-	Y	Y
Data storage	-	Y	Y
Data backup and recovery	-	-	Y
Meeting regulatory compliance	-	-	Y
Meeting Industry compliance	Y	Y	Y

Table 1: CC Benefits for Different Types of Business Organizations
Note: - denotes that the benefit is not significant.

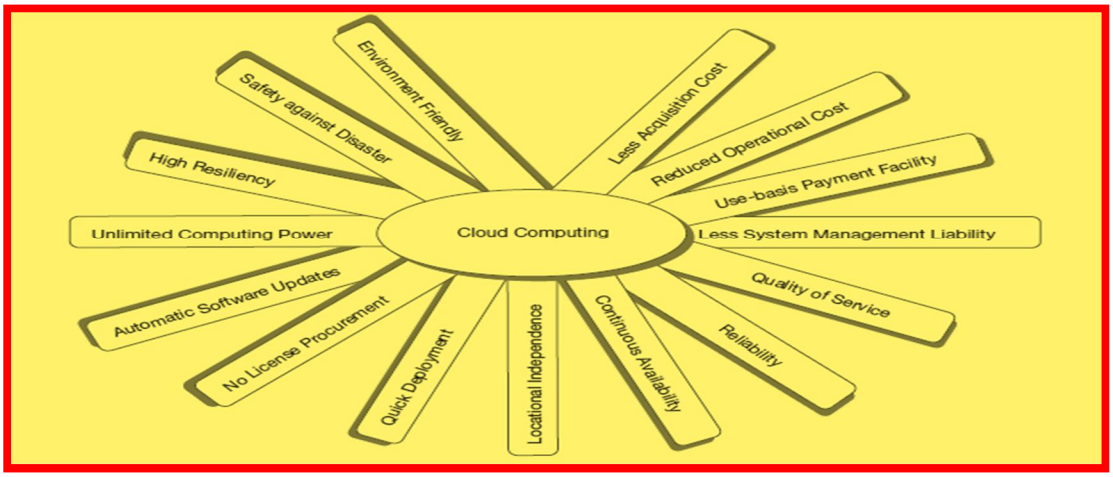


Figure 8: Advantages of cloud computing

©IJRASET: All Rights are Reserved

Murgesan and Bojanova also pointed to certain limitations that the consumers need to think about before they move to CC: (1) need of both reliable and always available high speed; (2) sometime slow response to increased traffic or uncertainties on the network or excessive load on computers in the cloud; (3) vulnerabilities concerning security of data and processing;(4) unauthorized access to user's data; (5) loss of data due to cloud failure ; and (6) reliability and continuous accessibility to services provided cloud service providers [7]. Last but not the least, Hashizume and others warns about some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues relating to compliance, privacy and legal matters. They point to the 'great deal of uncertainty' about security at all levels (e.g., network, host, application, and data levels). Therefore, they contend that 'Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving beyond their data center's network under their control. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization are secureand they can meet their service-level agreements, and that they can prove compliance to auditors' [26]. In an empirical study Garrison and others collected data in 2011 from a global sample of 314 companies in various industries and the study shows that the success of CC depends on realizing the importance of consumers' 'technical, managerial, and relational capabilities for leveraging cloud-computing resources to maximize the likelihood of deployment success and competitive advantage'. Thus they conclude that "that prior to implementing cloud computing, any potential client organization should assess its technical andmanagerial capabilities, as well as its ability to develop positive relationships with IT providers. The extent these capabilities are (or are not) developed determines how well cloud services achieve the organization's goals and potential competitive strategy" [27]. It is relevant to mention that there are differences between traditional IT model and new CC model comprehend elements complexity in the latter. Table 3 illustrates this [28]. It is apparent that the traditional IT differs from the CC in several

No.	Factors	Description	Most Affected Sectors
1	Technology Readiness (IT Resources)	Evaluate the readiness of existing technologies in the organization	Health Care, Higher Education, Public Sector
2	Human Readiness	Assess the readiness of staff to use cloud computing and their level of IT knowledge	Health Care, Higher Education, Public Sector
3	Organization & Top Management Support	Assessing the support of top management and the ability of the organization as a whole	Health Care, Higher Education, Public Sector
4	Environment	Assess the state of around especially external such as advances in technology, demand and competition	Health Care, Public Services, Public Sector
5	Security & Privacy	See the challenges and problems of privacy and risk management during the implementation of cloud computing	Health Care, Higher Education, Public Sector
6	Cost Saving	Reduction of operating costs and savings in IT management and any related tasks	Health Care
7	Interaction & Feedback	Measure feedback and effective communication of its implementation, especially to get the information fast and quick	Higher Education
8	Speed of Internet & Accessibility	In view of the speed of the internet and the ability of this technology gives access to users	Higher Education

Table 2: Factors in CC Implementation

©IJRASET: All Rights are Reserved

Traditional IT	Cloud Computing
• Hardware is hosted on the premises of the organization and/or manage hosted. • Hardware and software is provisioned for peak demand. • Service management monitoring is used to generate forecasts of demand usage and current SLA performance. • Chargebacks and compensations are used to adjust usage and payments. • Under-provisioning and over-provisioning of capacity can result from unforeseen demand changes. • Business invests in ownership of assets that can be enhanced and extended through IT programs and development. • Changes to IT involve migration and divestment/investment issues and programs.	• Hardware and/or software is hosted off-premise (public or hybrid) or on-premise as a private Cloud service. • Services are provisioned and used based on actual demand, providing this elasticity as a managed service. • Services are typically focused on short-term "burst" demand to gain cost savings over provisioning and owning the assets. • Statistical automated scaling is used to optimize the shared virtual assets. • Risk is transferred from the buyer to the seller/provider of the Cloud service. • Cloud sellers and providers seek to grow amortized economies of scale through increasing the numbers of users of the shared resources. • The IT infrastructure and operation is masked from the service user. Cloud is more than just SaaS.

Table 3: Traditional IT and Cloud Computing Features

Respects. CC is indeed a 'transitional model' consistent with the transitional era in which industrial era is transmuting into the era of post-industrial or information or knowledge society, to which attention will be given in the next section. In the new paradigm of CC the relationships between the consumer and the provider become a priority with a clearly defined 'contractual relationships and responsibilities. Benefits of the 'economies of scale' are used and applied as the advantage of size with priority parameters of price, know-how, and the like' [29].Operationally speaking, CC provides three types of service and fourdeployment models [30], as shown in Table 4. Briefly, Software as a Service (SaaS), sitting at the top of the service models, does not require software and hardware facilities and also its customers do not control components, security and applicationcustomization. SaaS providers are Google Docs, Microsoft Office 365, Salesforce Com., etc [22] [25]. In the Platform as a Service (PaaS) customer need to know how much processing unit memory or storage they require for installing applications, while they are provided necessary resources—software, hardware, operating system, server, deployment tools and database etc. –by the service providers such as Amazon Web Services, Google App Engine, and Microsoft azure [22]. In the Infrastructure as a Service (IaaS), embodying the virtualization concept, enables the consumer to use its infrastructure such as processing, storage, networks, etc, provided by the service providers. One example of IaaS is Amazon EC2. [22] [31]. As said earlier, there are four deployment models. Private cloud infrastructure is basically for exclusive use by business organizations. Private cloud service has more data security, more energy efficiency, and more reliability [22] [31]. Public cloud Infrastructure is available to many consumers but is owned by the service provider. Services are offered over the internet but this type of services has security and privacy issues. Community cloud deployment provides services to various consumers of a community and can be located on -premise or off-premise. 'The goal of community cloud deployment is to provide the benefits of public cloud, like multi-tenancy, pay-per-use billing etc. to its consumers along with added level of privacy and security like the private cloud' [12]. The hybrid cloud if formed is a combination or two or more organizations, enabling them to share storage of critical applications and data, and also to better handle data and security concerns of the concerned organizations. [12] [22]. Fernandes et al. advance that cloud service models along with chosen servicing models have security requirements which the businesses should assess each models before adopting one of them. There are six requirements such as identification and authentication, authorization, confidentiality, integration and non-repudiation, and availability. For instance, 'authorization requirements on IaaS, PaaS, and SaaS models on public cloud are mandatory to prevent unauthorized access to its assets' [32]. Let me now pass on to the next section that portrays the emergence of Information/Knowledge society, accompanied by information economy /knowledge economy, both of which are embedded the Information and Communications Technologies (ICTs). Cloud Computing is one of several new technologies that are embodied in the ICTs. 'Cloud computing involves the use of computing and ICT resources that are delivered as a service over the Internet from geographically disparate locations, using a shared and dynamically scalable infrastructure [33].

©IJRASET: All Rights are Reserved

SERVICE MODELS	
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
DEPLOYMENT MODELS	
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Table 4: NISTCloud Computing Service and Deployment Models

©IJRASET: All Rights are Reserved

III. INFORMATION AND COMMUNICATION TECHNOLOGIES:THE RISE OF INFORMATION/KNOWLEDGE/DIGITAL SOCIETY AND ECONOMY

Since the 1970s a new technological paradigm – organized around ICTs – came into being and triggered revolutionary transformations in every sphere of life and society by what is now aptly called 'the information technology revolution', a pervasive event that changed the entire world in terms of its profound impact and its resultant consequences [34]. Technologically speaking, as Castells elaborates: 'A new world is taking shape at this turn of the millennium. It originated in the historical coincidence, around the late 1960s and mid-1970s, of three independent processes: the information technology revolution; the economic crisis of both capitalism and statism, and their subsequent restructuring; and the blooming of cultural social movements, such as libertarianism, human rights, feminism, and environmentalism. The interaction between these processes, and the reactions they triggered, brought into being a new dominant social structure, the network society; a new economy, the informational /global economy; and a new culture, the culture of real virtuality. The logic embedded in this economy, this society, and this culture underlies social action and institutions throughout an interdependent world' [35]. From a methodological viewpoint, this is not technologically deterministic, for, as pointedly emphasized by Castells, notbecause 'new social forms and processes emerge as a consequence of technological change. Of course, technology does not determine society. Nor does society script the course of technological change, since many factors, including individual inventiveness and entrepreneurialism, intervene in the process of scientific discovery, technological innovation, and social applications, so the final outcome depends on a complex pattern of interaction' [33] *Okinawa Charter on Global Information Society*, created at the Kyushu-Okinawa Summit in 2000, proclaims that the vision of an inclusive ' information society' (hereafter IS) which enable people to fulfil their potential and realize their aspirations through a the 'free flow of information and knowledge, mutual tolerance, and respect for diversity' . ICTs go a long way 'to create sustainable economic growth, enhancing the public welfare, and fostering social cohesion, and work to fully realize its potential to strengthen democracy, increase transparency and accountability in governance, promote human rights, enhance cultural diversity, and to foster international peace and stability'[36]. The European Council in its meeting of 2000 held a special meeting on 23-24 March 2000 in Lisbon and agreed on a new strategic goal 'to strengthen employment, economic reform and social cohesion' as part of a 'knowledge-based economy' [37]. The Spring 2003 *Report* of the European Commission noted how Europe was undergoing a transformation into a knowledge-based economy and society. It argues that 'the European Union is evolving into a post-industrial and knowledge-based society, just as two centuries ago Europe evolved from an agrarian into an industrial society. Production is shifting steadily from material and labour intensive products and processes to knowledge intensive ones. In this context, the key strategic resource for future prosperity has become knowledge itself. Knowledge-based societies and economies are based on the production, distribution and use of knowledge. Therefore, economic growth depends directly on investment in knowledge that increases the productive capacity of traditional factors of production, i.e. knowledge and resulting innovations raise the returns on and the accumulation of other types of investment'[38].

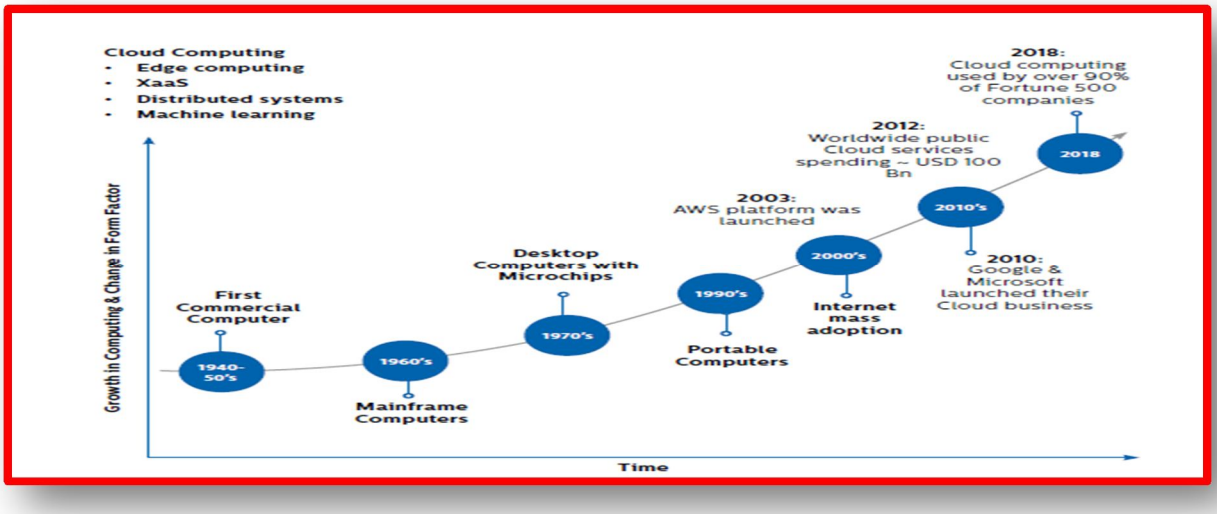


Figure 9: Technology's Evolution since 1960s – From Mainframesto Internet and Cloud computing and Beyond

©IJRASET: All Rights are Reserved

Before the concept of IS is defined and elaborated further, let me mention that cloud computing is a product of successive technological developments as shown in Figure 2. Figure 9 shows how CC and commercial internet arose over the years [39]. The paradigm of CC is basically based on the use of internet. The next Table 5 shows the leading technological ingredients that go into the making of information society and it includes the requirements of the process of digitization in the evolution and facilitation of the information society [40]. However, the leading characteristics and challenges of digitaltechnologies [41] are shown in Table 5. It is stated that cloud computing has 'actually triggered a paradigm shift in the provision of IT infrastructures and can therefore be regarded as a major driver of the digital revolution' [42]. The word 'digital' refer to 'the representation of physical items or activities through binary code. When used as an adjective, it describes the dominant use of the latest digital technologies to improve organizational processes, improve interactions between people, organizations and things, or make new business models possible' [43]. The word 'digital' should be distinguished from the concept of 'digitalization' which is relevant to CC business. Digitalization, according to Garner, refers to 'the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business' [44].Two concepts of digitization and digitalization should be differentiated. Digitization involves analog to digital conversion, as in converting a essay written on the paper into a PDF file or scanning a photograph. So digitization encodes the data in a digital format. Digitization has benefits since the data can be used to automate processes and facilitates better accessibility. In contrast, 'Digitalization moves beyond digitization, leveraging digital information technology to entirely transform a business' processes — evaluating, reengineering and reimagining the way you do business. If digitization is a conversion of data and processes, digitalization is a transformation. More than just making existing data digital, digitalization embraces the ability of digital technology to collect data, establish trends and make better business decisions' [45]. For instance, having analysed the relevant data collected by an internet device to find out new sources of revenue, one may use the same collected data to advise the farmers how to enable them to maximize their yields or productivity. As Urbach and Röglinger summarize: 'While digitization covers the technical process of converting analog signals a digital form, the manifold sociotechnical phenomena and processes of adopting and using digital technologies in broader individual, organizational, and societal contexts are commonly referred to as digitalization'. Digital technologies, which are driven by digitalization, include both emerging technologies like the Internet of Things (IoT) or blockchain and more established technologies such as social media, mobile computing, advanced analytics, and cloud computing (SMAC) and are characterized , in contrast to the earlier technology, by ' three characteristics: re-programmability, which separates the functional logic of a device from its physical embodiment, homogenization of data, which allows for storing, transmitting, and processing digital content using the same devices and networks, and a self-referential nature yieldingpositive network externalities. Digital technologies can be further classified with respect to whether they involve humans actively or passively, how they treat data, whether their input and output is purely digital or can also be physical, or whetherthey serve infrastructural or application-oriented purposes....In sum, digital technologies enable platforms, autonomous products, sensor-based data collection, analytical insight generation, as well as analytical and augmented interaction [46].

'Information and Communication Technologies (ICTs)encompass all those technologies that enable the handling of information and facilitate different forms of communication among human actors, between human beings and electronic systems, and among electronic systems. These technologies can be sub-divided into:	
1	Capturing technologies, with input devices that collect and convert information into digital form. Such devices include keyboards, mice, trackballs, touch screens, voice recognition systems, bar code readers, image scanners and palm-size camcorders
2	Storage technologies, producing a variety of devices to store and retrieve information in digital form. Among these are magnetic tapes, floppy disks, hard disks, RAM disks, optical disks (such as CD-ROMs), erasable disks and smart cards (credit-card sized cards with memory and processing capacity for financial transactions or medical data).
3	Processing technologies,creating the systems and applications software that is required for the performance of digital ICTs
4	Communications technologies,producing the devices, methods and networks to transmit information in digital form. They include digital broadcasting, integrated services digital networks, digital cellular networks, local area networks (LANs), wide area networks (WANs, such as the Internet), electronic bulletin boards, modems, transmission media such as fibre optics, cellular phones and fax machines, and digital transmission technologies for mobile space communications (the new Low Earth Orbit satellite voice and data services).

©IJRASET: All Rights are Reserved

5	Display technologies,which create a variety of output devices for the display of digitized information. Such devices include display screens for computers, digital television sets with automatic picture adjustment, set-top boxes for video-on-demand, printers, digital video discs (which might replace CD-ROM drives and audio CD players), voice synthesizers and virtual reality helmets.
Today the common feature of these ICTs is digitization.Digitization is the process through which information (whether relayed through sound, text, voice or image) is converted into the digital, binary language computers use. Computers cannot understand information in the form of pictures or words, but only when it is broken down into binary digits or bits: .zero. or .one., .yes. or .no., .on. or .off.. The conversion of information into this form makes it possible to transmit information from different sources through one channel and to reduce the risks of distortion. Thus the use of the digital language facilitates the convergence of computers, telecommunications, office technologies and assorted audio-visual consumer electronics. Their integration, in turn, allows information to be handled at higher speed, with more flexibility, improved reliability and lower costs'.	

Table 5: Components of ICTS and Digitization

DIGITAL TECHNOLOGIES		
NO	CHARACTERISTICS	CHALLENGES
1	Cross-platform functionality--content can be accessed across multiple devices, particularly via cloud services	Battery-- life battery durability diff ers from device to device
2	Mobility--staying online anywhere, anytime	Insecurity--many sites and apps may not be secure and personal data might be abused
3	Dynamism--continually evolving and impacting users	Privacy--a more open practice raises significant privacy issues
4	Personalisation--creation of a personalised digital environment	Scalability--to optimise content for mobile applications more attention has to be paid to the amount of data that moves back and forth on each page; images have to be adjusted and/or removed, if possible, and layout adjusted for the most popular devices
5	Connectedness--becoming part of a global community of peers, e.g. via social networking sites	Quantity--since the Internet provides a vast amount of information, precise search and retrieval might be difficult
6	Ubiquity--ubiquitous computing can occur usingany device, in any location and in any format	Intrusiveness--communication via a variety of channels available online, 24/7 connectivity
7	Robustness--most devices nowadays are powerful and reliable	Quality--the quality of sources and resources varies enormously; digital literacy skills are required to assess the validity and relevance of information
8	Interactivity--the web as an interconnected, two-way space, rather than a passive consumption space	Time consuming--online presence is engaging and takes time
9	Intuitivity--most sites and applications/apps areuser-friendly	Triviality--it is a challenge to filter out the large amount of irrelevant and meaningless information and 'noise' on the Internet
10	Openness--social and participatory media makeinteractions more visible and promotable,e.g. digital scholarship/e-research.	Training--navigating digital technologies and harnessing the power they afford is a skill to be acquired
11	---	Cost--while many resources and tools appear to be free, there is usually a cost involved, whether in advertising or inthe device used to access the resources
12	---	Unreliability--sometimes apps or websites crash or are hacked
13	---	Transitoriness--sites are constantly developing and adapting; a site orinterface one has got used to may suddenly change
14	---	Connectivity--ubiquitous access means that when we are not connectedproblems might occur as people expect 24/7 connectivity

Table 6: Characteristics and Challenges of Digital Technology

©IJRASET: All Rights are Reserved

Furthermore, digitalization profoundly impacts business and society since the technologies enable innovative business models such as 'the platform based models of well-known companies including AirBnB, Uber, or Facebook, ordecentral models enabled by blockchain and 3D printing' and bought about 'changes industry structures such as reduced entry barriers make technology-savvy start-ups flourish and digital giants such as Google or Apple push forward to manifold sectors... In our opinion, the most significant characteristics of digitalization are not the usage of data or adoption of technology, but the unprecedented speed of change and level of connectedness, which also facilitates the customers' dominant role as well as the convergence of the physical and the digital world' [46]. The information society is thus inclusive of digital technologies, as shown earlier in the emergent ICT ecosystem [1] The information society is the outcome of the Third Industrial Revolution, as shown in Figure 2. The role of cloud computing gradually emerged as a new paradigm in the Fourth Industrial Revolution while remaining, if not strengthening, the social structure of the Information society. CC became recognized as a new technological paradigm in the IT domain and also became the driver of what is called 'a major driver of digital revolution' [47]. Many argue that ICTs, along with other heartland technologies such as biotechnology, nanotechnology, and materials technology, are causing 'a global technology revolution' or a 'Third Industrial Revolution' at an accelerating speed and setting forth, in the words of Freeman and Perez, a new 'techno-economic' paradigm'[48 [49].

What is information (IS) and/ or knowledge society (KS)? To begin with, the *World Summit on the Information Society* in 2003 in the *Geneva Declaration of Principles* acknowledged its common desire and commitment 'to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on thepurposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights' [50]. The World *Summit on the Information Society (WSIS*), in Tunis (2005) reaffirmed its 'desire and commitment to build a people-centred, inclusive and development-oriented Information Society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights, so that people everywhere can create, access, utilize and share information and knowledge, to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals' [51]. In the year, 2005 Government of India constituted its own National Knowledge Commission (NKC) 'to "*leapfrog in the race for social andeconomic development"* for establishing a knowledge-oriented paradigm of development to achieve its own information and or knowledge society goals such providingaccess to knowledge, building knowledge concepts, promoting knowledge creation, encouraging knowledge application ,and investment in Knowledge Services [52]. *Report on Europe and the GlobalInformation Society: Recommendations of the High-level Group on the Information Society to the Corfu European Council*, known as *Bangemann Report* (1994), state that information and communications technologies are generating a new industrial revolution already as significant and far-reaching as those of the past resulting in the rise of the information society. 'It is a revolution based on information, itself the expression of human knowledge. Technological progress now enables us to process, store, retrieve and communicate information in whatever form it may take - oral, written or visual - unconstrained by distance, time and volume. This revolution adds huge new capacities to human intelligence and constitutes a resource which changes the way we work together and the way we live together' [53]. Against this backdrop, it is to be noted that the concept of information society, along with a host of other allied or similar concepts came to the forefront of theoretical discourse from the 1970s and 1980s coinciding with the development of innovations and their diffusion of ICTs and digital technologies throughout the world. Becla suggests that concept was introduced by Tadlo Umeaso in 1963 who defined the IS as 'the society getting informed through the computer' [54]. In 1966 Robert Lane argued that we live in a "knowledgeable society" of 'knowledgeable society' or 'the age knowledge' in the context of policy making changes [55]. In 1968 Brzezinski spoke of 'Technetronic Society' – 'A society that is shaped culturally, psychologically, socially, and economically by the impact of technology and electronics, particularly computers and communications' [56]. In 1968 A. Etzioni drew attention to 'Active Society'in which he spoke of transitions of all societies in the'post-modern' period which witnessed the 'expansion of man's knowledge' [57]. Around 1960 Drucker talked about 'knowledge Work' and 'knowledge worker' and later in 1993 spoke of 'the shift to knowledge society' and stated that 'the basic economic resource - 'the means of production' to use the economist's term - is no longer capital, nor natural resources (the economist's 'land'), nor 'labour'. *It is and will be knowledge'* in the post-capitalist society hinting at the coming of information and/or knowledge society [58]. Nora and Minc(1980) envisioned an IS in France and elsewhere due to the merging pervasiveness of *telematique*, the convergence of telecommunications with computers and data processing. In the computerized society - information is 'socialized', that is, 'promoting the preparation of data on the basis of which the strategy of the center and the desires of the periphery may reach agreement whereby Society and the State not only

©IJRASET: All Rights are Reserved

support each other but produce each other' [59]. This points to the triumph of the envisaged good society in the coming of computerized future. Another social analyst, Touraine traced in 1969 the emergence of 'post-industrial society' as programmed society superseding earlier the industrial society [60].

One of the most leading proponents of the supersession of the industrial society by 'post-industrial society' was Bell who attempted to explain 'an axial change in the social structure (defined as the economy, the technology and the stratification system) of the society'. In wake of the rise of telecommunications 'a new social framework became decisive for the way in which economicand social exchanges are conducted, the way knowledge is created and retrieved, and the character of the occupations and work in which men engage. This revolution in the organization and processing of information and knowledge, in which the computer plays a central role, has as its context the development of what I have called the post-industrial society' [61]. Thus, for him, IS is embodied in post-industrial society, Bell's preferred label. In the anniversary edition of his classic book *The Coming of Post-Industrial Socie*ty (1999), he specifically highlighted theses dimensionsof post-industrial society: (1) '*The centrality of theoretical knowledge' in which 'the* codification of theoretical knowledge and materials science becomes the basis of innovations in technology. One sees this primarily in the new science-based industries—computers, electronics, optics, polymers—that mark the last third of the century'; (2) '*The creation of a new intellectual technology* which means that 'through new mathematical and economic techniques—based on the computer linear programming, Markov chains, stochastic processes and the like -- we can utilize modeling, simulation and other tools of system analysis and decision theory in order to chart more efficient, "rational" solutions to economic and engineering, if not social, problems'; (3) '*The spread of a knowledge class'* by which Bell refers to 'the technical and professional class'; (4) '*The change from goods to services'* such as 'primarily human services (principally in health, education and social services) and professional and technical services (e.g., research, evaluation, computers, and systems analysis)'; (5) '*A change in the character of work'* which is 'primarily a"game between persons" (between bureaucrat and client, doctor andpatient, teacher and student, or within research groups, office groups,service groups)' and this points up 'a completely new and unparalleled state of affairs';(6) '*The role of women'* who for the first time have 'a secure base for economic independence'; (7) '*Science as the imago'* for science has become inextricably intertwined not only with technology but with the military and with social technologies and societal needs. In all this—a central feature of the postindustrial society—the character of the new scientific institutions—will be crucial for the future of free inquiry and knowledge'; (8) '*Situses as political units*' consisting of 'four *functional* situses—scientific, technological (i.e., applied skills:engineering, economics, medicine), administrative and cultural—and five *institutional* situses -- economic enterprises, government bureaus, universities and research complexes, social complexes (e.g., hospitals, social-service centers), and the military'; (9) '*Meritocracy*' 'based on achievement, through the respect of peers'; (10) '*The end of scarcity?'* . In the post-industrial society, 'there will be scarcities of information and of time. And the problems of allocation inevitably remain, in the cruder form, even, of man becoming *homo economicus* in the disposition of his leisure time'; and finally (11) '*The economics of information*' which is by its nature 'a collective, not a private, good (i.e., a property'. Its implication is that postindustrial society requires that a "competitive" strategy between producers is to be preferred lest enterprise become slothful ormonopolistic' and also 'a "cooperative" strategy in order to increase the spread and use of knowledge in society' [62]. Bell's typology of different societies isdescribed in Table 7 below [63]. The heightened emphasis on information and/or knowledge in his work is what makes Bell's contribution to the concept of information society central. This is also why different theorists include Bell in their analysis of information society [64] [65] [66] [67] [68] [69] [70] [71].

There is no consensus over the exactness and contours of what the IS is. Luc Soete defines it as a society that is 'currently being put into place, where low cost information and data storage and transmission technologies are in general use. This generalisation of information and data use is being accompanied by organisational, commercial, social and legal innovations that will profoundly change life both in the world of work and in society generally' [72]. Webster, who is critical of the concept's validity, opines that information society can be defined along five dimensions: 1 technological; 2 economic;3 occupational;4 spatial; and 5 cultural. The dimensions are not, however, mutually exclusive [64]. Van Dijk looks at the IS from the viewpoint of changing *substance* of activities and processes He gives a comprehensive definition: "In an information society the information intensity of all activities becomes so high that this leads to: 1. an organization of society based on science, rationality and reflexivity; 2.an economy with all values and sectors, even the agrarian and industrial sectors, increasingly characterized by information production; 3. a labour market with a majority of functions largely or completely based on tasks of information processing requiring knowledge and highereducation (hence, the alternative term *knowledge society*);4.a culture dominated by media and information products with theirsigns, symbols and meanings.Itis the intensity of informationprocessing in all these spheres that allows usto describe it as 'a new type of society'[73]. Mansell and Steinmueller 'utilize the term 'information society' to refer to statements about the useof information and communication technologies and the related social, economic, political, and culturaldevelopments linked to the

©IJRASET: All Rights are Reserved

growing availability of new forms of information and means of communication'[74]. According to Cardoso, the IS, though based on exchange of information as its *'central and predominant social activity'* can be defined *'as a process of social change based oninformation,* which itself is the expression of human knowledge. The informationsociety is fruit of the technological process that enables us toprocess, store, select and communicate information in all forms availablein it – oral, written and visual – without distance, time or volume-relatedrestrictions – giving the human being new capacities and changing the wayin which we live and work together' [75]. Dordick and Wang define the IS as 'one in which society is aware of the importance of information in every aspect of its work, an attitude of mind that makes for the efficient, productive, broad utilization of information in every aspect of life' [76]. For Feather, the IS implies a society as an outcome of 'the product of the use of computer and audiovisual media' [**77**]. It is a sober truth that the concept of the IS, however real empirically, is elusive, try as one might to define it. Be that as it may, a generalized conception of the IS can be derived from Bell's work [78] in the Table 8. For Bell the IS signals the 'an explosion of information' in everyday life in the wake of'the creation, ownership and distribution of information' resulting in the emergence of information industries that contribute to the 'the gross national product (GNP) of a country' [78]. No less important is that fact that there are advocates as there are critics [64] [79][80] [81] of the IS. Hassan [**82**] provides a summary of the contentions on the substances of the IS between the two conflicting groups in the following Table 9.

Mode of Production	Preindustrial Extractive	Industrial Fabrication	Postindustrial Processing; recycling
Economic Sector	Primary	Secondary	Services
	Agriculture, Mining, Fishing, Timber, Oil, and Gas	Goods-Producing, Manufacturing, Durables, Nondurables, Heavy Construction	Tertiary Transportation, Trade, Utilities Quaternary Finance Insurance Quinary Real Estate Health, Education Research, government, Recreation
Transforming Resource	Natural Power Wind, Water, Draft animal, Human Muscle	Created Energy Electricity-oil, gas, coal, nuclear power	Information Computer and data-transmission systems
Strategic Resource	Raw Materials	Finance Capital	Knowledge
Technology	Craft	Machine Technology	Intellectual technology
Skill base	Artisan, manual worker, farmer	Engineer, semi-skilled worker	Scientist, technical and professional occupations
Methodology	Common sense, Trial and error, Experience	Empiricism, experimentation	Abstract theory, models, simulations, decision theory, systems analysis
Time Perspective	Orientation to the Past	Ad hoc adaptiveness, experimentation	Future orientation: forecasting and planning
Design	Game against nature	Game against fabricated future	Game between persons
Axial principle	Traditionalism	Economic Growth	Codification of theoretical knowledge

Table No: 7 Comparison of properties of Three Historical Societies
The Preindustrial, Industrial and Post-industrial Societies

©IJRASET: All Rights are Reserved

FEATURES OF INFORMATION SOCETY	
1	Information becomes increasingly important as the economic, cultural andpolitical resources upon which the emerging global information economyand information societies are organized, with the majority of occupationsbased upon information or knowledge work.
2	The dynamic innovation of ICTs is seen to be transforming the potential forprocessing, storing and transmitting of information in ways previouslyunimaginable and ICTs are thereby becoming more pervasive in our lives.
3	Electronically networked economies and societies fundamentally transformour conceptions of time and space, enabling information flows to transcendtemporal and physical boundaries and thereby facilitate processes ofglobalization and networking enterprise.
4	Information becomes culturally more prevalent through multimedia applications, but also more contested and less meaningful, in a world ofcompeting, contradictory and constantly changing images, signs andmessages.

Table 8: Information Society

CONFLICTUAL PERSPECTIVES ON THE INFORMATION SOCIETY			
	Focus	Advocates	Critics
1	Economic Relations	More skilled workforce, flattened hierarchies, empowered consumers, more profitable businesses	Economic dualism, deskilling of middle classes, 'information proletariat'
2	Employment	More leisure time, more knowledge-based jobs, greater efficiencies and flexibilities	Trades and skills lost to ICTs, 'downsizing' by employers, and widespread job insecurity
3	ICTs and democracy	Two-way, decentralized political communication, emergence of 'electronic democracy'	Neoliberal domination, widespread political apathy, growth of state corporate surveillance
4	Global dimension	'Global Village' and the' technological leapfrogging' of Third World countries, i.e., China, India	Domination by corporate capitalism, exacerbation of global inequality in development of economic power
5	Information and culture	Vast expansion of access to information, the centrality of the internet, 'networked communities'	'Information without meaning', loss of 'real' community, dominance of Anglo-American cultural imperialism
6	Space and time	End of 'tyranny of distance', rational coordination of global business, time-savings of ICTs	'Tyranny of the moment', lack of reflective 'slow' time, superficial and hurried cultural forms

Table 9: Contrasting Perspectives on the Information Society

Leaving that aside, the IS is a contemporaneous reality accompanied by different prevailing discourses on the IS. It has been discussed in detail by Targowski [83] who provides a typology of the IS in Table 10. It is also useful to elucidate in a tabular form different dimensions and with indicators of Knowledge Society, as provided by Dragomirescu and. Sharma [84] in Table 11. This forcefully sheds quite a light on the nature, scope and role of the KS in a national society framework. It is more concretely supplemented by the role ICTs play in transforming societies into sustainable societies realizing the UN sponsored 'millennial goals' [85]. As a matter of fact, information society, as evident from Bell's, analysis, contains the ingredients of knowledge society (KS). Waters states that, while following Bell, 'the post-industrial society is a knowledge society. In a knowledge society science and technology become intimately related because technology is driven by theoretical as opposed to practical knowledge; and the shares of employment of GDP in the knowledge field become relatively large' [86]. Indeed, IS evolves into a knowledge society and economy meaning thereby that in KS knowledge is productively exploited. Furthermore, Blasi contends that knowledge society matures into he calls 'wisdom society'. The rationale behind this logic is that, while knowledge is a conscious utilization of information, 'wisdom' refers to one's choice of his behaviour based on knowledge and shared values – a choice that enhances the collective well-being and awareness about social consequencesof individual 'action'

©IJRASET: All Rights are Reserved

IS Type	Paradigm	Purpose	Main Information Solution	Measures Per 1,000 population
Data (Dossier)	Measurement	Reduction	Mechanization and Automation, Off-line systems	Number of data entry personnel
Computer	Measurement	Reduction	Automation and How to compute? Off-line systems	Number of computers
Mass Media	News	Dissemination	Printing	Number of newspapers and Number of TV sets
Networked	Connection	Exchange	Internet, Intranet Networked enterprise	Number of Internet Users, Number of Intranet servers
Virtual	Electronic presence	Exchange and Opinion	Internet, Intranet Virtual enterprise systems	Number of bulletin board systems (national and organizational)
Informative	Optimization	Decision-making	What to process? Data mining Online systems Application Portfolio	Number of OLAP software per organization, % of GDP spent on IM, % of I-workers in the labor force
Communicate	Familiarity	Planning	Networking Online systems Networked enterprise	Number of Internet users, Number of telephones, Number of TV sets and Number of newspapers, % of GDP spent on telecomm.
Knowledge	Rules	Understanding	Research, education Information retrieval	Number of scientists Number of professors, Number of students
Robotized	Rules	Decision-making	Automation of judgment	Number of expert systems
Informed	Awareness	Decision-making	Data mining Networking Enterprise-wide systems	Number of OLAP software, and Mass Media and Network Indexes, Free press
Learning	Understanding	Planning and acting	Computer-aided instruction, Information retrieval Digital library	Number of published books, Number of digital books and scientific documents
Global	Justice	Operations	Virtual government Global systems	Number of applied virtual global agencies
Self-sustainable	Optimization	Survival	Green economy Ecological systems	Amount of energy from renewable sources
Monitoring	Warning	Survival	Satellites or tam-tam drums	Number of served people

Table 10: The paradigms and measurements of information societies

If this materializes the knowledge society can evolve into a wisdom society. 'To build up a "wisdom society", in which there is a wise and wide use of knowledge – as there must be in a modern learning society – it is necessary … to develop, in a balanced way, the scientific and economic dimensions in each person, together with the creative and spiritual dimensions' [87]. Without being technologically deterministic, the ICTs with their creative potential become tools designed and implemented by thepeople thus accelerating the transition of IS to KS in historically specific social, economic, political, cultural and technological contexts [88]. There are, however, theorists who prefer, not the term IS or KS, but the concept of what is called 'network society'. For instance, Castells says that "the network society, in the simplest terms, is a social structure based on networks operated by information and communication technologies based in microelectronics and digital computer networks that generate, process, and distribute

©IJRASET: All Rights are Reserved

information on the basis of the knowledge accumulated in the nodes of the networks'. Network society brings along its certain features such as network sociability, networked individualism, and networked state [89]. Van Dijk suggests that 'the network society concept emphasizes the form and organization of information processing and exchange. An infrastructure of social and media networks takes care of this. So the network society can be defined as a social formation with an infrastructure of social and media networks enabling its prime mode of organization at all levels (individual, group/organizational and societal). Increasingly, these networks link all units or parts of this formation (individuals, groups and organizations). In western societies, the individual linked by networks is becoming the basic unit of the network society. In eastern societies, this might still be the group (family, community, work team) linked by networks' [90]. ICTs gave rise to the

A multi-dimensional scorecard of the Knowledge Society at national level		
Pillars	Dimensions	Proxy indicators
Education and training	Higher education	public spending on higher education; tertiary education attainment; tertiary graduates in mathematics, science and technology; GDP share invested in higher education
Innovation systems	Training, Research & development	lifelong learning participation , patent intensity; citation impact of country's scientific output; scientific publications highly cited in patents; receipts of royalty and license fees; R&D employment; Creativity Index
	Net knowledge inflows	international trade in core cultural goods; international trade in ICT goods; technology balance of payments; share of trade in high-tech products; international mobility flows of foreign tertiary students; net migration of skills
	Knowledge networks	composition of telecentre networks; university industry R&D centres; academic spin-offs; R&D consortia; research sub-contracting; patent citations
	Shared spaces For knowledge creation	co-patents and co-publications; fairs, exhibitions digitised cultural heritage; household expenditure on civic amenities (culture, entertainment
Information and Communications Infrastructure	ICT accessibility	Network Readiness Index; B2B and B2C sales in e-commerce; broadband Internet subscribership; hosts and websites on the Internet; Internet domain name registrations
	Role of mass media	entertainment and media market: voice & accountability; press freedom
Economic and institutional regime	Rule of law consistent with international norms	Corruption Perceptions Index; Global Peace Index
	Political vision & strategy	Country's Project Maturity Index; political stability; regulatory quality; government effectiveness
	Human rights & freedom	Human Development Index; Index of Personal and Economic Freedom; EIU Democracy Index
	Intellectual property	Cyber law coverage; rate of piracy in digital intellectual goods
	Business environment that rewards innovation	high-tech companies benefiting from early-stage venture capital investment; venture capital investment for private R&D; Index of Economic Freedom; Business Competitiveness Index

Table 11: A multi-dimensional scorecard of the Knowledge Society at national level

©IJRASET: All Rights are Reserved

SUSTENABLE DEVELOPMENT GOALS (SDG)	ADVANCED ICTS CONTRIBUTTION TO ACHIEVING SDG
Goal 1: End poverty in all its forms everywhere	ICTs help businesses to become part of the formal market economy; provision of better price information helps increase revenues and profits; mobile banking provides access to loans and microcredit; mobile payment systems reduce transaction costs; computer modelling and simulation can help develop better policies
Goal 2: End hunger, achieve food security and improved nutrition and promote sustainable agriculture	Smart agriculture solutions to monitor soil and weather conditions allow increasing crop yield; better coordination of food supply chains reduce waste; better crop management can restore soil conditions and create more sustainable agriculture
Goal 3: Ensure healthy lives and promote well-being for all at all ages	IoT allows innovative forms of low-cost health monitoring and diagnostics; ICTs can connect remote health workers with specialized diagnostic services; big data analytics allow forecasting of disease outbreaks
Goal 4: Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all	ICTs allow access to online educational resources and learning communities; big data analytics help identify learning challenges and create more effective instruction, and allow continuing education and specialized training
Goal 5: Achieve gender equality and empower all women and girls	ICTs can provide women access to empowering information and education, and access to microcredit and secure payment systems
Goal 6: Ensure availability and sustainable management of water and sanitation for all	Smart water management reduces losses; water quality monitoring enhances water safety; smart waste management reduces risks of contamination
Goal 7: Ensure access to affordable, reliable, sustainable and modern energy for all	Smart metering and smart appliances allow better energy use management; microgrids and smart grids allow for building more sustainable energy supply while lowering the carbon footprint; green buildings reduce energy consumption
Goal 8: Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all	IoT and artificial intelligence have significant potential to increase productivity and economic growth while reducing the resource intensity and carbon footprint of production; additive manufacturing provides new opportunities for smaller scale, custom manufacturing
Goal 9: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation	ICT, IoT, big data and artificial intelligence contribute to smarter infrastructures; preventative maintenance and continuous monitoring increase resilience; the plasticity of advanced ICTs allows accelerated learning, rapid prototyping and continuous innovation
Goal 10: Reduce inequality within and among countries	Advanced ICTs will allow further decentralized and localized production with the potential to reduce income inequality among countries; by improving education, they can contribute to reducing interpersonal inequality within countries
Goal 11: Make cities and human settlements inclusive, safe, resilient and sustainable	IoT applications allow creating smart and energy-efficient cities; big data analytics and artificial intelligence can help in creating better urban transport systems, safer neighbourhoods and more accountable city government
Goal 12: Ensure sustainable consumption and production patterns	ICTs in combination with IoT and big data analytics can improve coordination between consumers and producers; additive manufacturing and just-in-time production will increase efficiency and sustainability
Goal 13: Take urgent action to combat climate change and its impacts	Big data analytics and artificial intelligence can help reduce the carbon footprint of production and consumption; information sharing and learning communities can develop and replicate better practices
Goal 14: Conserve and sustainably use the oceans, seas and marine resources for sustainable development	New sensing and monitoring technologies can help track oceanic resources; big data and artificial intelligence will facilitate better resource management practices and will allow early warning systems
Goal 15: Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss	Monitoring of the use of land resources, deforestation, and soil conditions can contribute to the preservation of resources
Goal 16: Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels	Big data analytics combined with open data policies can empower citizens; monitors and big data analytics may help in increasing government transparency; direct trade relations may increase global tolerance and understanding
Goal 17: Strengthen the means of implementation and revitalize the global partnership for sustainable development	ICTs enable the formation of new communities of engaged citizens; big data analytics and artificial intelligence will allow advanced modelling of developments that can be shared rapidly and widely

Table 12: Utilizing advanced ICTs to pursue SDG

©IJRASET: All Rights are Reserved

'digital' [91] space and platform and at the same time made possible the emergence of Information Economy and/or Knowledge economy and Digital economy possible - latter being a narrower concept and also gradually becoming wider making the society digital[92]. Digital technologies have penetrated into manifold 'dimensions of everyday life, affecting family and intimate relationships, leisure activities, paid work, education, commerce and the ways in which mass media are presented and consumed'[92]. Because of digital technologies' ubiquity and pervasiveness it is now accepted that 'life is digital' [93]. Information economy now refers to 'the broad, long-term trend toward the expansion of information- and knowledge- based assets and value relative to the tangible assets and products associated with agriculture, mining, and manufacturing' [94]. Knowledge economy (KE), more specifically speaking, uses knowledge as the key engine of economic growth. It is an economy in which knowledge is acquired, created, disseminated, and used effectively to enhance economic development. Contrary to some beliefs, the concept of the knowledge economy does not necessarily revolve around high technology or information technology (IT). ..The successful transition to a knowledge economy typically involves elements such as making long-term investments in education, developing innovation capability, modernizing the information infrastructure, and having an economic environment conducive to market transactions' [95][96] [122]. ODI offers Table 13 which describes the functions of KE [97]. Johansson and other define digital economy as 'referring specifically to the recent and still largely unrealised transformation of all sectors of the economy by the general spread of ICTs'. [98].Similarly, according to Brynjolfsson and

KNOWLEDGE ECONOMY		
'A Knowledge Economy is one that utilises knowledge to develop and sustain long-term economic growth, thus the Knowledge Economy framework focuses on four pillars which it suggests are needed to support a successful knowledge economy'.		
PILLARS OF KNOWLEDGE ECONOMY		FUNCTIONS AND CONTRIBUTIONS
1	Economic and Institutional Regime	It enables the creation, diffusion, and utilisation of knowledge and provides incentives that encourage the use and allocation of existing and new knowledge efficiently. The economic environment requires good policies and must be favourable to market transactions, (viz. free trade and foreign direct investment). The government needs to protect property rights to encourage entrepreneurship and knowledge investment.
2	Well-educated and skilled Population	This creates, shares, and uses knowledge efficiently. Education, especially in the scientific and engineering fields, is essential to accomplish technological growth. A more educated society in this regard is likely to engender more technologically sophisticated, generating higher demand for knowledge.
3	Information infrastructure	It facilitates the communication, dissemination, and processing of information and technology. The increased flow of information and knowledge worldwide thus reduces transactions costs, producing greater communication, productivity and output in the end.
4	Innovation system	An efficient innovation system of firms, research centres, universities, think tanks, consultants, and other organisations is required to promote, apply and adapt global knowledge to local needs to create new technical technology leading to higher productivity growth.

Table 13: Knowledge Economy: Pillars and Functions

Kahin the term 'digital economy' refers 'specifically to the recent and still largely unrealized transformation of all sectors of the economy by the computer-enabled digitization of information ... In its broadest conceptualisation this emergence of a digital economy can be viewed as an evolutionary process whereby the economy and all its sectors are being transformed by the rapid development, adoption and use of ICTs innovations. In this respect ICTs functions as a new generic general purpose technology, which impacts society both broadly and deeply by giving rise to a wide array of new products, production processes and services' [94]. The ability of the ICTs to create, organize, manipulate transmit, store and perform on information in digital form promoting quality of life as well as economic development, leaving aside many other aspects as shown in Table 14 [99]. Atkinson and states 'the digital economyrepresents the pervasive use of IT (hardware, software, applications and telecommunications)in all aspects of the economy, including internal operations of organizations (business, government and non-profit); transactions between organizations; and transactions between individuals, acting both as consumers and citizens, and organizations' [99].

©IJRASET: All Rights are Reserved

Another view is that , knowledge economy is 'a state of economic being and a process of economic becoming that intensively and extensively leverages knowledge assets and competences as well as economic learning to catalyze and accelerate sustainable and robust economic growth'[100]. Coined since the 1990s, the segments, components and actors of digital economy have been described by UNCTAD *Report* (2019), as shown Figure 10 and Table14 [101]. The 2015 ITU *Report* notes that 'the cloud computing market has likewise grown rapidly, driven by vast data-storage capacities and increasingly by applications in the cloud, allied with flexible user devices. Data-traffic volumes have been drivenby higher bandwidth applications, particularly video, while big-data storage and analysis has become very big business, it being estimated that the volume of data generated in digital format is doubling every two years. The Internet of Things is rapidly becoming a reality and machine-to-machine (M2M) communications are also expected to grow significantly. All of these developments illustrate the continued dynamic growth of ICTs, which have the potential to transform other social and economic sectors' [101] It was borne out by the fact most cloud traffic is generated, as part of the digital economy, in the USA, Asia Pacific and Western Europe, which is altogether 90% of all cloud traffic. The share of the top five providers such as Amazon Web Services (AWS), Microsoft, Google, IBM and Alibaba in the global cloud infrastructure services market is more than 75 per cent, with AWS alone accounting for over a third of that market [102]. Cloud computing, along with other technologies, is setting the contemporary trends in digital economy, making possible 'the future of "smart everything" (i.e. grids, homes, business processes, energy, healthcare, transport and government), as well as empowering businesses, consumers and society at large....Collection of data will be facilitated by the expansion of machine-to-machine (M2M) communications with large-scale processing delivered by "cloud computing" services. New data analytics will be able to process and analyse large volumes of data, frequently termed "big data". These phenomena together form the 'building blocks of smart networks'' [103]. Cloud computing, along with IoT, and AI are becoming 'the new drivers of the ICT ecosystem' [85] as illustrated in Figure 11. Related to cloud computing within the ICTs and digital technologies is the phenomenon of universal diffusion of the internet across the world. Castells opines that the Internet is the technological basis of the organizational form in the Information Age of the information and/or knowledge or network society. Indeed, 'the Internet with large-scale processing delivered by "cloud computing" services. New data analytics will be able to process and analyse large volumes of data, frequently termed "big data". These phenomena together form the 'building blocks of smart networks" [103]. Cloud computing, along with IoT, and AI are becoming 'the new drivers of the ICT ecosystem' [85] as illustrated in Figure 11. Related to cloud computing within the ICTs and digital technologies is the phenomenon of universal diffusion of the internet across the world. Castells, opines that the internet is the technological basis of the organizational form in the Information Age of the information and/or knowledge or network society. Indeed, 'the Internet is the fabric of our lives. If information technology is the present-day equivalent of electricity in the industrial era, in our age the Internet could be likened to both the electrical grid and the electric engine because of its ability to distribute the power of information throughout the entire realm of human activity'[104]. It is a cliché to say the internet has permeated our lives in unprecedented ways, and the individual has now become a digital citizen in the emergent digital society [105]. Along with the computer, the Internet- a worldwide network of computers - has emerged as a 'technological behemoth' [106], as shown in Figure 12 [107]. Figure 13 shows the timeline of the growth of the Internet between 1965 and 2018 [108]. Total number of internet users in 2019 were 4.9 billion, which is an increase of 366 billion (9%) versus January 2018. 3.48 billion people used social media in 2019 and the world wide total growth amounted to 288 million (9 percent) since 2018. On mobile devices 3.26 billion people used social media in January 2019, and the growth in this use of social media was more than 10% which is in figure 297 million of new users [109]. It is also reported that the global penetration rate of the internet went up from nearly 17 per cent in 2005 to over 53 per cent in 2019 [110]. The following Table 15 depicts how internet, occupying the central position in the defining digital society of the Information age [111], has developed its own economy: 'the economic activities that either support the Internet or are fundamentally dependent on the Internet's existence'. According ting to Dutton "information economy refers to 'an economy in which the processing and transmission of information is a central activity' [141]. Figure 14 depicts the internet economy. It has three domains that are as follows: First, its applications and services define the contours of the experiences of Internet users and enable them to 'communicate, share, and innovate'. Second, access provision which enables internet users to connect to and communicate through the ICTs throughout the world. Third, service Infrastructure describes different services and businesses that enable the users to mutually connect with each other eventually creating and maintaining the internet. 'It includes specialised services like naming and addressing management, hosting and distribution of content, and the interconnection of the networks themselves. A number of the large platform companies are increasingly investing in cloud services and content delivery networks (Amazon Web Services) to undersea cables (Google), extending their reach from the application layer into the services and infrastructure layers'. Moreover in the internet economic market place, given the dynamic nature of the internet and the growing share of the big businesses(viz. AWS, Google, Microsoft, Alibaba) in the market, cloud computing is also on theincrease. Its marketing services like IaaS and

©IJRASET: All Rights are Reserved

PaaS is expected 'to almost triple to $110.8 billion in 2021 from $41.9 billion in 2016. The current top 10 providers are expected to increase their market share even further, to 70% from 50%, by 2021' [112]. The ubiquitous nature of the internet in everyday life, can be best put in the words of Fuchs [113]: 'On the Internet, we searchfor information, plan trips, read newspapers, articles, communicate with others by making use of e-mail, instant messaging, chat rooms, Internet phone, discussion boards, mailing lists, video conferencing; we listen to music and radio, watch videos, order or purchase by auction different goods, write our own blogs, and contribute to the blogs of others; we meet others, discuss with others, learn to know other people, fall in love, become friends, or develop intimate relations; we maintain contact with others; we protest, access government sites, learn, play games, create knowledge together with others in wikis, share ideas, images, videos; we download software and other digital data, and so forth. On the Internet, we also can feel being lost, disoriented, dissatisfied, scared, bored, stressed, alienated, lonesome, and so forth'[113]. Finally, Table 15 exhibits how internet empowers people [114]. In this regard Government of India is also moving forward to developing India as a digital society and economy since 2018 when **it** approved the National Digital Communications Policy-2018 (NDCP), which 'envisions India's transition to a digitally empowered economy and society, through the establishment of ubiquitous, resilient and affordable digital communication infrastructure and services. It seeks to unlock the transformative power of digital communication networks and attempts to outline a set of goals, initiatives, strategies and intended policy outcomes'. It aims at (1) ensuring access to broadband for all;(2) creating four million additional jobs in the digital communication sector; (3) enhancing the contribution of the digital communication sector to 8% of India's GDP;(4) propelling India to the top 50 nations in the ICT Development Index of ITU;(5) enhancing India's contribution to global value chains; and (6) ensuring digital sovereignty. It seeks to achieve these goals by 2022 [115].While discussing the complexities in the concept of 'information integrity' in this era under discussion Rogerson cryptically remarks that 'the Information Age offers so much but only if we master the technological keys to the informational Pandora's Box' [116]. He was in all probability referring to problems, vulnerabilities, and risks embedded in the concept of information integrity in general and information/knowledge, digital society in particular. In fact problems, vulnerabilities and risksincluding, 'security', 'data security' and 'privacy' in the information society – including both two behemoths of computer and internet -- have attracted attention of many analysts [117][118][106] [119] [120] [121] [122] [123]. It is these aspects that I take up in the following section.

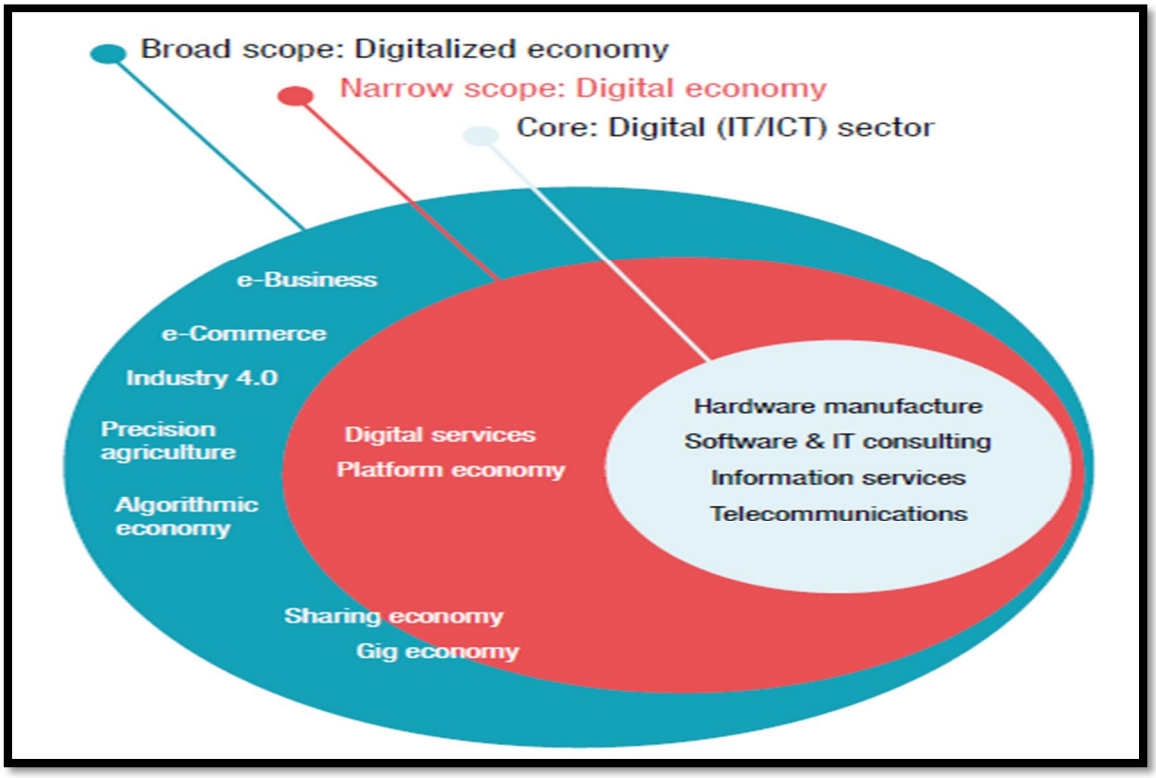


Figure 10: Segments of Digital Economy

©IJRASET: All Rights are Reserved

DIGITAL ECONOMY COMPONENT	ACTORS				ECONOMY-WIDE IMPLICATIONS
	Individuals (as users / consumers and workers)	MSMEs	Multinational enterprises / digital platforms	Governments	
Core, digital sector	• New jobs for building and installing ICT infrastructure. • New jobs in telecom and ICT sector, especially ICT services.	• Greater inclusion under suitable circumstances or spillovers/domestic linkages. • Increased competition from cloud-service providers.	• Investment opportunities for companies that meet high capital, technological and skills requirements.	• Attracting investment. • Tax revenues from the economic activity created.	• Increased growth, productivity and value added. • Employment creation. • Investment and diffusion of technologies; R&D likely located in high-income countries. • Mixed trade impacts.
Digital economy	• New jobs in digital services, especially for highly skilled people. • New forms of digital work, including for the less skilled.	• New opportunities in digital ecosystems. • Increased competition from foreign digital firms.	• Enhanced productivity from data-driven business models. • Greater control of value chains using platform-based business models. • New opportunities in the sharing economy.	• More tax revenue resulting from increased economic activity and formalization of enterprises. • Lost customs revenue from digitalization of products.	• Higher growth, productivity and value added. • Employment creation/losses. • Higher investment. • Aggregation of digital firms in some locations. • Mixed trade impacts. • Market concentration.
Digitalized economy	• New jobs in ICT occupations across industries. • Need for new skills as higher-value roles are redesigned using digital tools. • Greater efficiency of services received. • Job losses or transformation due to digitalization. • Risk of worsened working conditions. • Improved connectivity. • More choice, convenience, customization of products for users and consumers. • Lower consumer prices.	• Platform-enabled market access. • Reduced transaction costs. • Risk of "race to the bottom" in markets vs. ability to find a niche. • Lost opportunities due to automation (e.g. logistics, business processes). • New roles in service provision. • New business opportunities for digitalized enterprises.	• Emergence of platform firms with data-driven models. • Gains from efficiency, productivity and quality. • Opportunities for the monetization of data. • Increased competitive advantage to digital platforms. • Increased market power and control of data value chain. • Leading digitalization in different sectors.	• Increased efficiency of services through e-government. • Increased revenue from customs automation. • Unclear impact on tax revenue: increases from higher economic activity; losses from tax optimization practices by digital platforms and MNEs. • Data-driven opportunities to meet various SDGs.	• Growth through improved efficiency in sectors and value chains. • Productivity improvements. • Innovation impacts. • Potential crowding out of local firms in digitally disrupted sectors. • Potential automation in low- and medium-skill jobs. • Wider inequality. • Mixed trade impacts. • Impacts on structural change.

Table 14: Digital Economy Components and Actors

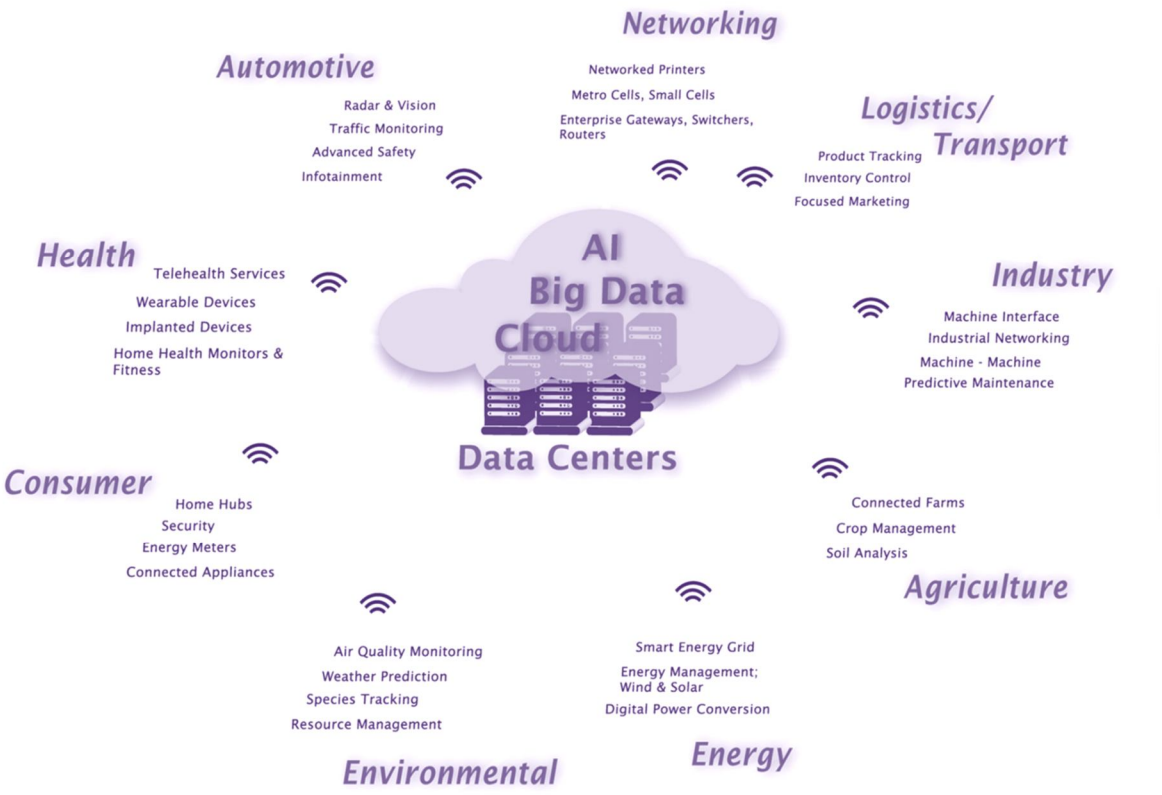


Figure 11:Cloud computing,IoT, Big Data and Artificial Intelligence asthe new drivers of the ICT ecosystem

©IJRASET: All Rights are Reserved



Figure 12: Internet and attached social and other websites

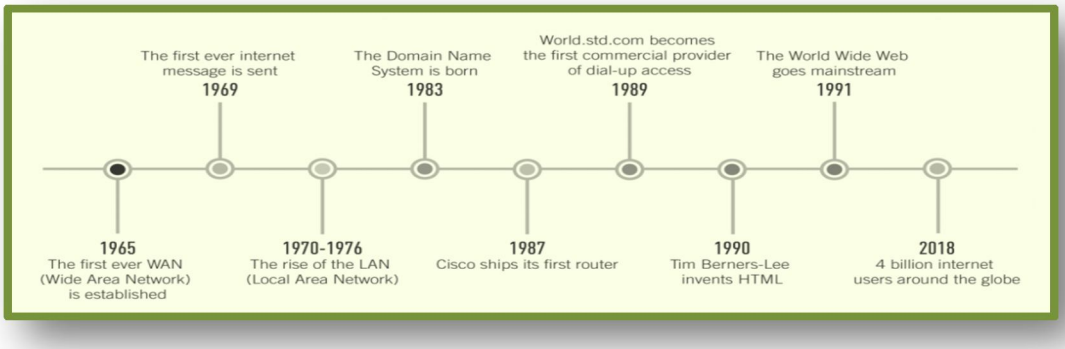


Figure 13: Timeline of the Internet

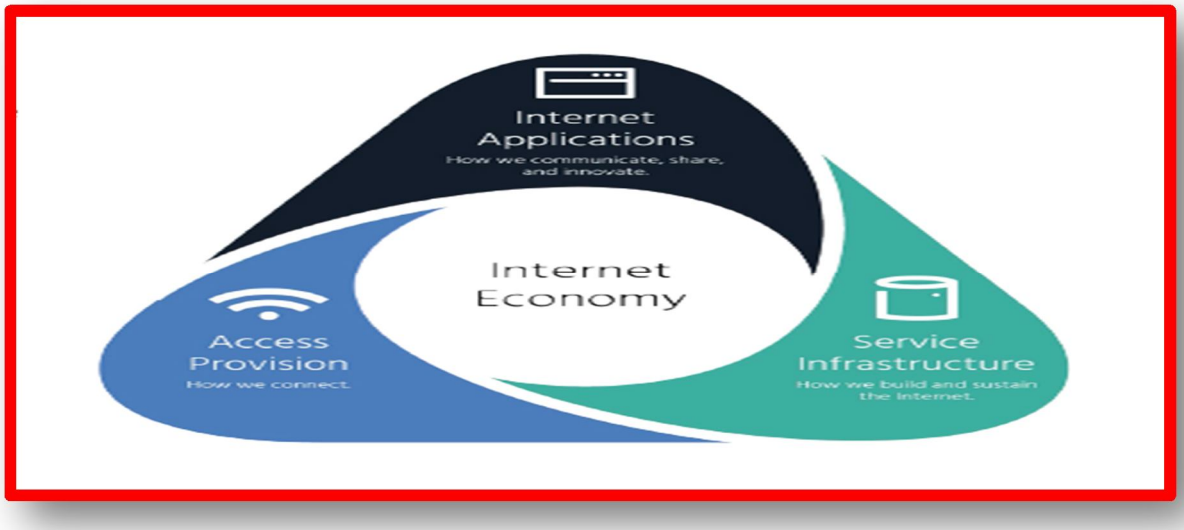


Figure: 14 Internet Economy

©IJRASET: All Rights are Reserved

Dimensions of Empowerment by Internet		
1	The ability to Connect	It ensures connectivity from anywhere to anywhere independent of technical and other impediments. This enhances 'the Internet's value as a platform for innovation, creativity and economic opportunity'.
2	The ability to Speak	It ensures the use of the internet for private, secure and — when proper — anonymous communications in safe and secure manner as a medium of self expression.
3	The ability to Innovate	It ensures that the individual or organisation hasthe ability, free from any restrictions, 'to develop and distribute new applications and services', for anyone who wants to use them.
4	The ability to Share	It ensures, inconformity to the principle of 'fair use, and thefreedom to develop and use open source software', sharing, learning and collaboration (viz. 'the open development of the key components of the Internet, such as the Domain Name System(DNS) and the World Wide Web').
5	The ability to Choose	It ensures, given the free choice and transparency for accessing the internet, the users to gain control of their internet experience and contribute to 'the availability of better, cheaper, and more innovative Internet-related services'.
6	The ability to Trust	It ensures the user's trust on the internet to connect, speak, innovate, share and choose provided the internet is backed up by 'requisite security, reliability and stability of the network, applications and services'.

Table 15: Empowerment by Internet

IV. SECURITY, DATA SECURITY AND PRIVACY IN CLOUD COMPUTING IN THE INFORMATION/KNOWLEDGE/ DIGITAL SOCIETY

Cloud computing, an integral component of the information society in the scheme of the ICTs as a 'promising direction', is essentially a means of delivering computing and storage services over the Internet from any place across the globe [124] [125] [112]. In this CC has organic link with data, information, and knowledge, if not also wisdom, although the relationship among them are complex and here interpretations vary [126] [127] [128][129][130]. In any case they are all interrelated hierarchically, as shown in the Figure 15. Data can be defined as 'the lowest level of entity that is used in a system for processing matters of meaning concerning things'. Data contains information, which is the significance of the data, and is the 'vehicle for shifting information around'. Information is becomes knowledge when integrated with other information about the observed phenomenon, which enables the observer to increase understanding of the instance of the observed phenomenon through the observations that have been made'. Finally, wisdom refers to the 'ability to judge the appropriateness of action and to behave in the correct manner in a situation' [131]. They can be described in a rather simple manner. Data are 'discrete, objective facts or observations, which are unorganised and unprocessed, and do not convey any specific meaning'. Information is 'data that have been shaped into a form that is meaningful and useful to human beings'. Knowledge is 'data and/or information that have been organised and processed to convey understanding, experience, accumulated learning, and expertise as they apply to a current problem or activity'. Wisdom is 'accumulated knowledge, which allows you to understand how to apply concepts from one domain to new situations or problems' [127]. What is more important from the viewpoint the present discourse is the phenomenal significance of data for the IS and/or KS.The nature and character of this society with launch of the World Wide Web in 1989 and its rapid development made it possible to generate large volume of data that can be collected, stored, and analysed electronically. The term 'data explosion'--'increasingly vast amounts of structured, unstructured, and semi-structured data being generated minute by minute' – became a commonplace in the relevant literature. On the basis of a recent worldwide study by IBM, Holmes(2017) reports that 'about 2.5 *exabytes* (Eb) of data are generated every day. One Eb is 10^{18} (1 followed by eighteen 0s) bytes (or a million *terabytes* (Tb)'.The large scale data generated in the digital age came to be known as Big Data, which now refers 'not just to the total amount of data generated and stored electronically, but also to specific datasets that are large in both size and complexity, with which new algorithmic techniques

©IJRASET: All Rights are Reserved

are required in order to extract useful information from them. It led to birth of Data Science which is extremely important for business in particular since 'data in all its forms has the potential to provide a wealth of useful information if we can develop ways to extract it'. Data became the 'new oil', a phrase attributed to Clive Humby, i.e. an asset that is valuable for industry, commerce and politics with the implication that 'data, like oil, is extremely valuable but must first beprocessed before that value can be realized' [132]. Big data has many applications (viz. LinkedIn, Twitter, Facebook, E-Commerce, Gmail, Yahoo Mail, Youtube, Skype, Weblogs, Wikipedia, etc,) and magnitude of the production of data can be noted by the fact that now 'more than 30,000 GB of data are generated every second with a great rate of acceleration'. Data Revolution has broken out and in this the internet is the 'ultimate as the source of data' [133]. And Fuchs and Chandler rightly points out that recently 'Big Data has become an important aspect of digital capitalism, leading to the emergence of a new dimension of Big Data capitalism' [134].The Figure 16 shows important dimensions of Data Revolution [135].Given the this, the society has undergone what is called 'datamization', moving 'from a society where we lived our lives in relative freedom from record or comment to a world where data is collected and stored about nearly every move we make' [136]. The amount of data, which Patrignani and other call 'digital universe', is doubling every two years. 'By 2020, it is estimated that it will have reached 44 Zettabytes (44 x10^{21} bytes). This information deluge contains not only data produced by sensors, but also the digital traces left by human beings – the logs o their digital lives' [137].

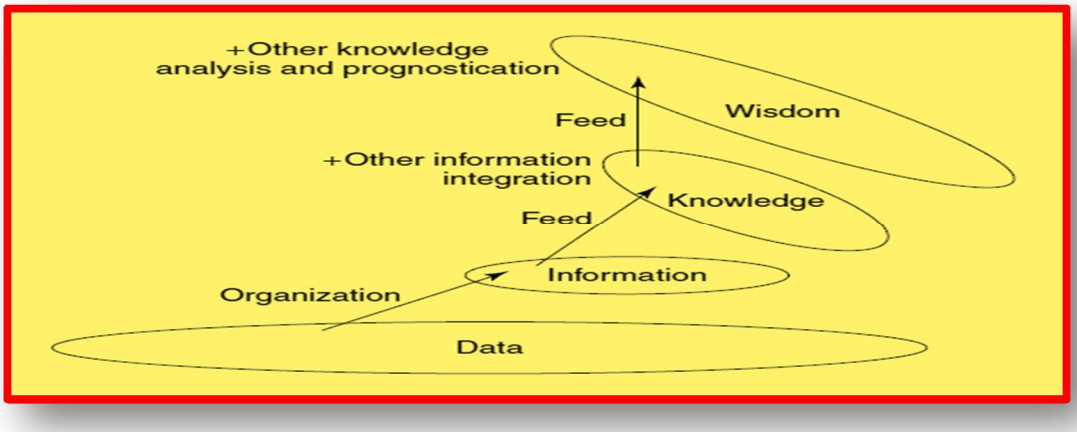


Figure 15: Representation of the relationship between
Data, Information, Knowledge, and Wisdom

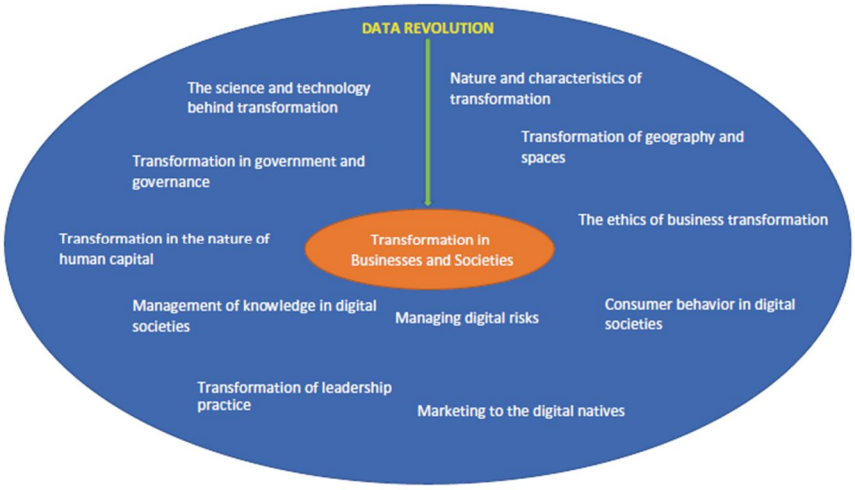


Figure 16: Data Revolution and its Different Dimensions

©IJRASET: All Rights are Reserved

Keeping the objectives of CC in mind, this is to note firmly that there has emerged a 'global data revolution' and individuals are now living 'undoubtedly in the data age' because 'from Twitter to the World Bank, the data revolution is transforming business as usual' [138].The data revolution, which is already reshaping how knowledge is produced, business conducted, and governance enacted, is based on 'the latest wave of information and communication technologies (ICTs) [139]. Simanowaski somewhat sarcastically says that we always loved data and information and quotes the title of a Berlin conference called Data Love (2011) giving its justification: "Today, data is what electricity has been for the industrial age. Business developers, marketing experts and agency managers are faced with the challenge to create new applications out of the ever-growing data stream with added value for the consumer. In our data-driven economy, the consumer is in the focus point of consideration. Because his behaviour determines who wins, what lasts and what will be sold. Data is the crucial driver to develop relevant products and services for the consumer'[140]. In view of the development of new technologies (viz. sensors, biometrics, cameras, and GPS) data has become entity that is 'everywhere' [142]. 'Connect to the Internet, and the data you produce multiplies: records of websites you visit, ads you click on, words you type. Your computer, the sites you visit, and the computers in the network each produce data. Your browser sends data to websites about what software you have, when it was installed, what features you've enabled, and so on. In many cases, this data is enough to uniquely identify your computer'[143]. In view ubiquitous datafication– 'transforming all things under the sun into a data format and thus quantifying them' – the digital society has become 'the Datafied Society' [144]. Digital technologies have brought about 'the datafication of everything: all aspects of life are now transformed into quantifiable data' [145]. To give an example, there has arisen a new data actor, the broker, whose breadth and depth of information about data astounding. 'They collect demographic information: names, addresses, telephone numbers, e-mail addresses, gender, age, marital status, presence and ages of children in household, education level, profession, income level, political affiliation, cars driven, and information about homes and other property. They collect lists of things you've purchased, when you've purchased them, and how you paid for them. They keep track of deaths, divorces, and diseases in your family. They collect everything about what you do on the Internet' [143]. The ubiquitous datafication, together with the internet, is creating, among other things, massive market for the growth of data-driven businesses, bringing out innovations in business models, and also transforming the information/digital economy [113] [146] [138] [147][148].'Today, data is what electricity has been for the industrial age. Business developers, marketing experts and agency managers are faced with the challenge to create new applications out of the ever-growing data stream with added value for the consumer. In our data-driven economy, the consumer is in the focus point of consideration. Because his behaviour determines whowins, what lasts and what will be sold. Data is the crucial driver to develop relevant products and services for the consumer' [140]. At the same time internet is simultaneously a disruptive and a constructive technology that has fundamentally transformed businessesand is generating 'a whirlwind of business creativity' in the wake of data revolution [120][135]. All this is conducive to efflorescence and dynamic expansion of CC, which is, however, hindered in view of its associated challenges including security and privacy [125][136] [143][149][150] [151]. Table 16 summarizes the key challenges ofCC including security and privacy along with the threats immanent in them, which produces reluctance among the prospective consumers to go for CC in the organizations[151]. Two points should be noted. First, concepts of security and privacy, though related are not the same. In CC set-up, important security challenges are 'data outsourcing, multi-tenancy, massive data, and intensive computation' while data/information face up to both security and privacy issues [151]. While security enables privacy protection from undesired or illegitimate interception, it alone cannot secure privacy even when security remains a fundamental requirement for guaranteeing data/information privacy protection. It means therefore that privacy is 'a much broader concept than security', although security is required for privacy protection. However, to enhance privacy protection something more is required such as legislations and necessary guidelines (viz. theHealth Insurance Portability and Accountability Act (HIPAA) in the United States of America (USA) and the European Union (EU) Data Protection Act) [152]. Thus, security is 'the practice of defending information and information assets through the use of technology, processes and training from: Unauthorized access, Disclosure, Disruption, Modification, Inspection, Recording, and Destruction'. But data/information privacy is focussed on 'on the use and governance of individual data—things like setting up policies in place to ensure that consumers' personal informationis being collected, shared and utilized in appropriate ways. Security concentratesmore on protecting data from malicious attacks and the misuse of stolen data for profit'. Hence, Table 17 shows theon additional difference between privacy and security [153]. The terms 'privacy' and 'security' are often interchanged and this accounts for why the differences between them should be maintained [154]. To recapitulate, security refers to 'confidentiality, integrity and availability', above all, of data and is 'being free from danger or threat', while privacy refers to 'the appropriate use of information' and 'to be free from being observed or disturbed by others'. 'Security is necessary but not sufficient for addressing privacy. Even the best security controlmechanism may not have any impact on privacy protection' [12]. The second point relates to the commonalities that are there between security and privacy, which mean that the two are integrally connected with each other

©IJRASET: All Rights are Reserved

although analytically the two concepts are quite distinct. Figure 17 illustrates this [155]. Let me pass on to the cloud data life cycle that are invariably related to the security and privacy issues which impinge on both of of them, This is so because when a data/information or privacy breach happens by way of unauthorized acquisition, access, use, or disclosure of the data/information, then data/information becomes affected [156]. The following Figure 18 illustrates the data life cycle in different processes of the CCenvironment, implying the specific stage in the evolution of the data establishes it value at that stage with resultant outcome for the next stage. No less important is the state of data in CC. Kacha and Zituni summarises three states of data. These are classified as follows. First, **data-at-rest** is means that it is in a stable state stored in storage media in the cloud. However, it is susceptible to such possible risks as (a) risks(viz. data theft, leakage and alteration) associated with storage media sharing among different users; (b) risks (viz. potential difficulty connected with jurisdiction} associated with data location which the user does not know; and (c) risks (viz. service provider sub-contracting to a third party or another provider without informing the client) associated with storage media reliability. Second, **data-in-transit** is data in motion travelling across the network in the cloud. Its security requires that data will not be intercepted, altered or replaced while it is in transmissionor moving in the cloud. If the data moves from the data owner to the cloud and on to the use, it creates the issues of perimeter security, which raises another challenge requiring perimeter security technique such as software defined perimeter (SDP) to handle the condition. Finally, **data-in-use** refers to viewing, reading or processing involving creation, transformation or deletion of data. This state is susceptible to different risks depending on where the process is in the cloud and who can have access. Solutions to these three state of data security is dependent onthe specific state of the data and include specific remedial measuressuch as encryption, access control, transparency of the service provider etc. in the appropriate situation.[157] [158]. Further, the three states of data and the security issues connected with them, is one of 'top concerns of data owners when moving to the cloud' [158] In Figure 19, Subramanian and Jeyaraj cites a list of the data security issues The data-in-rest includes the following issues: (1) Data Recovery (i.e., accessing the damaged and repairing the damaged file); (2)Data Remanence/Sanitization (i.e., erasure of the data at the end of the life cycle); (3) Data Backup (i.e., storing 3 copies in different storages to protect against potential attacks); (4) Data Isolation (i.e.. separation of sensitive data from non-sensitive data and isolating data from unauthorized users to avoid VM to VM attacks ensuring confidentiality through access control); (5) Data Segregation (i.e. complete separation between the cloud users in the virtual environment); (6) Data Lock-in (i.e., foiling the movement of data out of or into the cloud); (7) Data Location (i.e., storage of data in unknown location involving security, legal and regulatory compliance). Data-in-transit has two issues: (8) Data Lineage (i.e., tracing the origin of data); and (9) Data Leakage (i.e. leakage due to accessing data by a multi-tenant). Common issues in data-in-transit and data-in-rest: (10) Data Integrity (i.e. maintaining the data from unauthorized observation, modification or interference); and (11) *Data Provenance* (i.e., integrity plus computational accuracy) [159]. The point remains that data security is a major issue that bears on ensuring privacy. 'Data security becomes particularly serious in the cloud computing environment, because data are scattered in different machines and storage devices including servers, PCs, and various mobile devices such as wireless sensor networks and smart phones'[160].

Security challenges for cloud model			
No.	Security parameter	Security challenge	Security threat
1	Confidentiality	Outsourcing	Loss of control , Data leakage, Malicious employee, Stealing of data (physically)
		Multi-tenancy	Cross VM attack through side channels. Attack from malicious system administrator, Access to residual data. Misuse of data by third party
		Broad network access	Insecure media while data is in transit
2	Integrity	Data auditing by third party,	Data exposure to third party,
		Transparency of computations from user	Violation of certain policies/procedures
3	Availability	Cloud infrastructure sharing	DoS, DDoS, Bandwidth starvation,,Fraudulent resource consumption
		Outsourcing	Discontinuity of services, Data loss, Non-availability of data owing to dispute, Improper data deletion
		Cloud interoperability	Inability to use data
		Cloud infrastructure sharing	Fault isolation
4	Privacy	Outsourcing	Profiling of users, Sharing of personal data with third party
5	Accountability	Identity secrecy	Inability to track activity, Identity spoofing

Table 16: Security challenges for cloud model

©IJRASET: All Rights are Reserved

No.	Privacy	Security
1	Privacy is the appropriate use of user's information	Security is the "confidentiality, integrity and availability" of data
2	Privacy is the ability to decide what information ofan individual goes where	Security offers the ability to be confident that decisions are respected
3	The issue of privacy is one that often applies to aconsumer's right to safeguard their informationfrom any other parties	Security may provide for confidentiality. The overall goal of most security system is to protect an enterprise or agency
4	It is possible to have poor privacy and good security practices	However, it is difficult to have good privacy practices without a good data security program
5	For example, if user make a purchase from XYZCompany and provide them payment andaddress information in order for them to ship theproduct, they cannot then sell user's informationto a third party without prior consent to user	The company XYZ uses various techniques (Encryption, Firewall) in order to prevent data compromise from technology or vulnerabilities in the network

Table 17: Distinctions between Privacy and Security



Figure 17: Areas where security and privacy efforts work together



Figure 18: Data Life cycle

©IJRASET: All Rights are Reserved

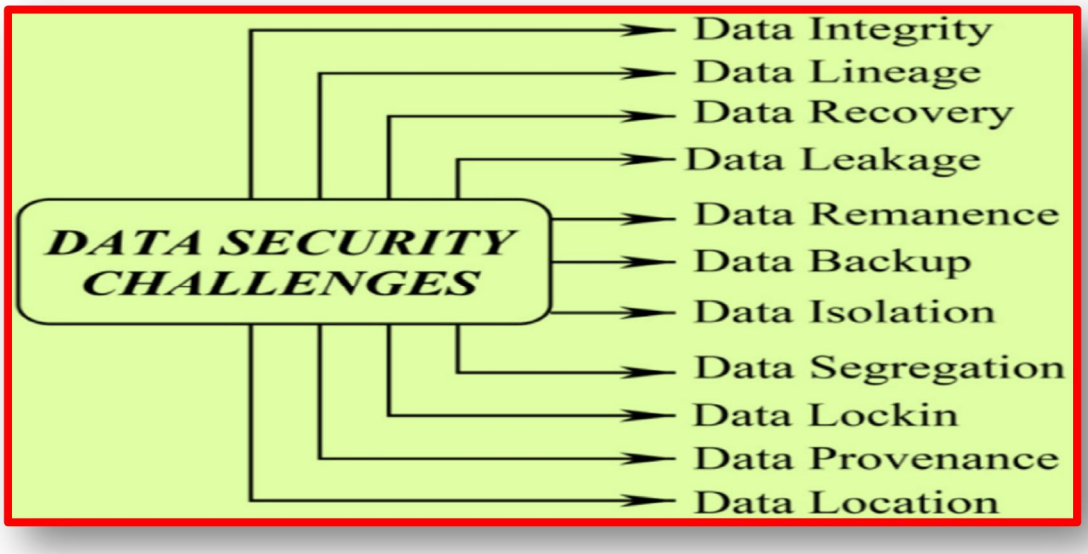


Figure 19: Classification of data related challenges

V. PRIVACY: MEANING AND ISSUES IN CLOUD COMPUTING

Protecting data and ensuring privacy is one of most challenging concerns or issues in CC and it is these which are responsible for the relative slowing down adoption of the CC by the individuals and business organizations [161] [162]. Data, as defined in the earlier section, can be classified into two categories. Private data, as Ghorbel and others exhaustively enumerate, can convey personally identifiable information (PII) such as (1) key attributes, namely individual's name, phone number, social security or national identity number, and passwords , all of which need to be removed when anonymization techniques are adopted; and (2) Quasi-identifiers , i.e. identifying attributes such as ZIP code, date of birth and address, which can be used to link anonymized dataset with other datasets enabling identification of individuals.

Data may also contain, more importantly, sensitive information which has been classified into such categories as (1) membership of different types of groups; (2) demographic characteristics like nationality, gender, educational level, job position, criminal records, etc.; (3) interests and habits indicating traceability, history of data usage, web browsing and shopping behavioural patterns, etc; (4) financial information such as credit card number, account balance, etc.; (5) health information such as medical record, disease, doctors' prescriptions, medical images etc., ; (6) hardware id indicating data subject's hardware identifiers like computer IP address, radio frequency identity (RFID) tags, MAC address, host name etc.; and (7) intellectual production concerning data subject's ideas, inventions prior to publication or validation [161]. This exhaustive list of information-contained data underscores very importance of privacy if such data slips out of data subject's control [163].

Trinckes, while dealing healthcare industry, concluded that 'privacy is more important than security because,without the abilityto be private in your own personal affairs, you are no longer secure.When businesses, the government, or even other people know *everything* about you—your actions, your thoughts, your feelings,your likes, your dislikes—you become a target. You can be manipulated and controlled' [164]. Defining privacy is like solving a conundrum, for there lacks blissful absence of consensus over the precise meaning and content of privacy.

There is no single all-agreed definition of privacy [165]. Solove points out that privacy is 'a concept in disarray'. Nobody can articulate what it means, for currently as 'sweeping concept' most theorists 'have frequently lamented the great difficulty in reaching a satisfying conception of privacy' [166]. Koontz quotes Nissenbaum who points to the same conclusionby saying that 'one point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject' [167]. In Table 18 Mulligan and others propose an analytical tool for mapping the claims for, criticisms of, and contests over privacy along the following 14 dimensions (viz. object, justification, contrast concept, exemplar, target, subject, action, offender, from-whom, mechanism, provider, social boundaries, temporal scale and quantitative scope and clustered the dimensions around a set of five 'meta-dimensions of *theory*, *protection*, *harm*, *provision* and *scope*'. They claim that analytically separating these threads helps clarify privacy's function and value in practice.

©IJRASET: All Rights are Reserved

This mapping reveals 'analytical discrimination so that one can recognize how different privacy conceptions are operating differently in different practical contexts' [168].

The Universal Declaration of Human Rights, 1948, in Article 12, declares that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' [169].

Weston, Who was aware of the alarms concerning the future of ' privacy in an age of computer data banks' defines privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others' [170] [171].

In *The Right to Privacy* Warren and Brandeis vented their frustration with the intrusions into individual privacy by prolific use of the latest technological innovations and accordingly tried to combat threat to individual privacy by 'adding a broad new right to the common law - the "right to be let alone" or "right to privacy", following what Judge Cooley's called this right 'to be let alone''[172] [173].

Nissenbaum advocated the protection of privacy in view of the fact that ' information and communications technology, by facilitating surveillance, by vastly enhancing the collection, storage, and analysis of information, by enabling profiling, data mining and aggregation, has significantly altered the meaning of public information' [174]. She accordingly proposed that 'privacy is neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information. The framework of contextual integrity ... makes rigorous the notion of appropriateness. Privacy may still be posited as an important human right or value worth protecting through law and other means, but what this amounts to is a right to contextual integrity and what this amounts to varies from context to context' [175].

Grodzinsky and Tavani applied 'Nissenbaum's model to Google Docs, as an example of a sociotechnical system/practice involving cloud storage. We believe that Google Docs conforms to the requirements of the decision heuristic within the framework of contextual integrity'. However, they also 'saw that there are other variations of cloud storage in which the practices used may not necessarily comply with these standards' [176]

. More importantly, Cloud Computing brought in new dimensional change in the meaning of privacy. Earlier end-consumers used to carry their documents around on disks, rather than on memory discs as it is now the case. CC changes the way in which information is now managed or data processing takes place.

End-users themselves access cloud services, the sharing of computing and storage resources on demand without knowing the underlying technology. Under the circumstances, without knowing where the data is or how the processing is done raises the issues of security, privacy and trust for them.

'Can cloud providers be trusted? Are cloud servers reliable enough? What happens if data get lost? What about privacy and lock-in? Will switching to another cloud be difficult?' [177].

Further, the cloud service providers can sell the end users' data without their consent , may use their personal data for advertisement for profit or a malicious tenant virtual machine (VM) can steal data [178]. ITU thus defines privacy as "the right to self-determination, that is, the right of individuals to 'know what is known about them', be aware of stored information about them, control how that information is communicated and prevent its abuse. In other words, it refers to more than just confidentiality of information. Protection of personal information (or data protection) derives from the right to privacy via the associated right to self-determination.

Every individual has the right to control his or her own data, whether private, public or professional' [177]. The basis of modern privacy laws and practices around the world refers to informational self-determination meaning thereby 'the right or ability of individuals to exercise personal control over the collection, use and disclosure of their personal information by others' [179]. Danezis and Gurses define privacy 'as avoiding making personal information accessible to a greater public. If the personal data becomes public, privacy is lost' [180].

Hasan and Zawoad define privacy at two levels. At the consumer level, privacy is 'the protectionand appropriate use of the personal information of customers to meet their expectations about its usage'. As far as business organizations are concerned, privacy is 'the application of laws, policies, standards, and processes by which personally identifiable information (PII) of individuals is managed' [178].

©IJRASET: All Rights are Reserved

PRIVACY DIMENSION	DESCRIPTION	INTERROGATION	EXAMPLE
Dimensions of Theory			
Object	That which privacy provides to those protected, i.e. privacy provides protected agents with X	'What's privacy for?'	dignity; control over personal information
Justification	The motivation and basis for providing privacy, i.e. privacy is justified because of X	'Why should this be private?'	individual liberty; social welfare
Contrast Concept	That which contrasts to privacy, i.e. that which is private is mutually exclusive with that which is X	'What's not private?'	public; open; transparent
Exemplar	The archetypal threat to this concept of privacy, i.e. privacy is violated by X	'What's an example?'	identity theft; intrusive surveillance; gossiping neighbours
Dimensions Of Protection			
Target	That which privacy protects, i.e. privacy protects things of type X '	'What's privacy about? Privacy of what?'	personal information; body or likeness; private space
Subject	Actor(s) or entity(ies) protected by privacy, i.e. privacy protects agent X	'Whose privacy is at stake?'	myself, my child; social groups (e.g. teens); roles (e.g. students)
Dimensions of Harm			
Action	The act or behaviour that initiates or constitutes a privacy harm, i.e. staring at him while he was dressing in the locker room violated his privacy	'What act violated privacy?'	Solove's four meta-harms (collection, processing, dissemination and invasion)
Offender	Actor(s) violating privacy, i.e. privacy violated by agent X	'Who violated privacy?'	government; business entity; peeping torn
From-Whom	Actor(s) against-whom privacy is a protection, i.e. privacy provides protection against agent X	'Who is privacy protecting against?'	everyone; Government; 'friends of friends'
Dimensions of Provision			
Mechanism	That which instrumental^ secures privacy, i.e. the lock on her door protected her privacy	'How is privacy provided?'	legal regulations; technical design; social norms
Provider	Actor(s) charged with securing privacy, i.e. the telecommunications provider was responsible for technically securing the privacy other communications	'Who is supposed to provide privacy?'	Government; business entity; technology
Dimensions of Scope			
Social Boundaries	That wherein privacy applies, i.e. privacy applies in domain, situation, field, or site X	'Where is privacy found?'	hospital or university; nation-state or globally
Temporal Scale	The time span at which privacy applies, i.e. privacy applies for a span of X time	'How long is privacy required?'	permanent; fixed expiration; variable expiration
Quantitative Scope	Extent of application of privacy, i.e. privacy should be applied with a scope of X	'How widely does privacy apply?'	universally as strict rule; casuistically as per-case

Table 18: Dimensions of Contests over Privacy

©IJRASET: All Rights are Reserved

What are the privacy challenges, issues or concerns? The answers vary because researchers differ among themselves in terms of their respective focuses and emphases. For instance, L. Arokiam and others mention seven challenges: (1) Access, (2) Compliance, (3) Storage, (4) Retention, (5) Destruction, (6) Audit and Monitoring, and (7) Privacy Breaches [181]. Hasan and Zawoad lists eight privacy issues: (1) TrustAsymmetry, (2) Legal Issue, (3) Insider Threats, (4)Data Outsourcing, (5) Access Control, (6) Secure Identity, (7)Need For Accountability, and (8) Cloud Forensics [178]. Bhowmik cites four basic areas of concern for privacy: (1) Access to Data, (2) Compliance, (3) Storage Location, and (4) Retention and Destruction [12].Ghorbel and others include four main issues: (1) The Lack of User Control,(2) The Dynamic Nature of the Cloud, (3) The Lack of Technologies to ensure the Compliance and User's Preferences, and (4) the Difficulty to Achieve Accountability in the Cloud Environment [163]. Sankarwar and Pawar enumerate three privacy issues: (1) Misuse of Cloud Computing, (2) Malicious Insiders, (3) Tans Border Data Flow and Data Proliferation, and (4) Dynamic Provision [182]. Joshi et al. specifies four data privacy issues of 'utmost importance': (1) Loss of Sensitive Data, (2) Theft, (3) Insecurity in Logical separated Space, and (4) Data Integrity and Availability [183]. Sun and other lists four data security and privacy issues such as data integrity, data availability, data confidentiality, and data privacy, all of which are related to both software and hardware [184]. Mather and others catalogue seven key concerns of in the CC, which are as follows: (1) access, (2) Compliance, (3) Storage, (4)Retention,(5) destruction, (6) Audit and Monitoring, and (7) privacy breaches [185]. Kalloniatis identified nine privacy related properties such as (1) Isolation, (2) Provenanceability, (3) Traceability, (4) Intervenability, (5) CSA Accountability, (6) Anonymity, (7) Pseudonymity, (8) Unlinkability, and (9) Undetectability and Unobservability [186]. Kitkowska and others identified seven dimensions of privacy concerns: (1) *insecurity,* (2) *exposure,*(3) *unauthorized access,* (4) *secondary use of data,*(5) *misuse of data,*(6) *distortion,* and (7) *interrogation*[187]. Finally, Table19 cites the CC features and related privacy concerns as asserted by Pearson [188]. It is evident that researchers attribute different weight to different issues, challenges or concerns according to their particular focus on the theme of privacy in their respective analysis. The basic requirements in the cloud environment include guaranteeing, other than privacy, confidentiality, integrity, availability,authentication, authorization, and accountability [189]. Many of the security requirements are connected with approved Madrid Resolution to ensure an universally binding agreement to take 'proactive measures, whereby States are encouraged to promote a better compliance with the laws applicable on data protection matters, and the need to establish authorities to guarantee and supervise the rights of citizens'. The purpose of the Resolution was 'to define a series of principles and rights that guarantee the effective protection of privacy at an international level, as well as to ease the international flow of personal data, essential in a globalized world. Among the basic principles that must govern the use of personal data, and which have inspired the document, we find those of loyalty, legality, proportionality, quality, transparency and responsibility; all of them arecommon to the different existing legal texts in the various regulations on the matter and enjoy wide consensus in their corresponding geographical, economic or legal application environments' [192]. Even then, the legal landscape in CC, as Dziminski and Gleeson conclude, remains 'in many ways quite cloudy itself' [193]. The Obama Administration was proactive in promulgating certain overriding principles for data protection as evident in its 2012 issuance of the report *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. 'In response to that report, the Federal Trade Commission issued a report titled *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* guiding companies to follow three general principles of (1) privacy by design; (2) simplified consumer choice; and (3) transparency. In examining those principles, it can be seen that perhaps the US and EU are not as far apart as to data protection as it would otherwise appear inmedia reports and other descriptions of the two policies' [193]. Even though a checklist for big organizations is available for taking care of the sources of security and legal aspects [194], the inherent nature and complexity, which is growing because of technological developments in the CC domain, the legal aspects continue to remain problematic. Pearson is not far off the mark when she says that 'from a legal and regulatory compliance perspective, several of the key characteristics of cloud computing services including outsourcing, offshoring, virtualization and autonomic technologies may be problematic, for reasons ranging from software licensing, and the content of service-level agreements (SLAs), to determining which jurisdiction's laws apply to data hosted 'in the cloud' and the ability to comply with data privacy laws. ... Autonomic aspects of cloud computing—like many of the other aspects mentioned above—are one of its assets but need to be tailored to be compliant with privacy and legal issues' [194]. In Table 20 Ruiz and Pedraza identify the legal risks along with security issues related to protection of data privacy [195]. Privacy concerns are very likely to remain there in the CC.

©IJRASET: All Rights are Reserved

No	Cloud features	Key related issues
1	Multi-tenancy	Data of co-tenants may be revealed in investigations, isolation failure, proper deletion of data and virtual storage devices
2	Complex, dynamically changing environment; data flows tend to be global and dynamic	Ensuring appropriate data protection, overlappingresponsibilities in data management, unauthorized secondary usage, vendor demise, lack of transparency
3	Data duplication and proliferation; Difficult to know geographic locationand which specific servers or storage devices will be used	Exacerbation of trans-border data flow compliance issues, detecting and determining who is at fault if privacy breaches occur
4	Easy and enhanced data access from multiple locations	Data access from remote geographic locations subject to different legislative regimes, subpoenas, access by foreign governments, 'idiot with a credit card'

Table 19:Cloud Features and Key Related Privacy Issues

1	Collection Limitation Principle	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2	Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3	Purpose Specification Principle	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose
4	Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.
5	Security Safeguards Principle	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6	Openness Principle	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller(i.e. "Data controller" means a party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored,processed or disseminated by that party or by an agent on its behalf.
7	Individual Participation Principle	Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them. within a reasonable time; ii. at a charge, if any, that is not excessive;iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and(b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
8	Accountability Principle	A data controller should be accountable for complying with measures which give effect to the principles stated above.

Table 20: Basic Privacy Principles of National Application

©IJRASET: All Rights are Reserved

Risks identified	Description	Security issues
Subpoena and e-discovery	In the event of the confiscation of physical hardware as a result of subpoena by law-enforcement agencies or civil suits, the centralization of storage as well as shared tenancy of physical hardware means many more clients are at risk of the disclosure of their data to unwanted parties	Availability, Privacy
Risk from changesof jurisdiction	Customer data may be held in multiple jurisdictions, some of which may be high risk. If data centers are located in high-risk countries could be raided by local authorities and data or systems subject to enforced disclosure or seizure	Availability, Privacy
Data privacy	It can be difficult for the cloud customer (in its role of data controller) to effectively check the data processing that the cloud provider carries out, and thus be sure that the data is handled in a lawful way. There may be data security breaches which are not notified to the controller by the cloud provider. The cloud customer may lose control of the data processed by the cloud provider. The cloud provider may receive data that have not been lawfully collected by its customer (the controller)	Privacy, Accountability
Licensing risk	Licensing conditions, such as perseat agreements, and online licensing checks may become unworkable in a cloud environment	

Table 20: Cloud Computing Legal Risks and Security Issues (ENISA)

VI. SECURITY AND PRIVACY RISKS OF CLOUD COMPUTING OR THE INFORMATION/ KNOWLEDGE/DIGITAL RISK SOCIETY? A DISCURSUS

It is not that attempts have not been made to ensure security or privacy or both in the CC. Indeed there have numerous attempts to secure privacy in the CC in particular. While recognizing that 'privacy is one of the biggest unaddressed issues' CC currently faces, Allison and Capretz introduced a new Privacy as a Service (PraaS) which is 'hosted by a trusted third party and tasked with the job of both monitoring for privacy violations and creating accountability through enforcement. Enforcement is only effective when coupled with appropriate legislation, which also must be addressed' [196]. Shabalala and others proposed 'a data privacy monitoring framework that enables the data owner to stay in control over their data, thereby providing the required transparency to comprehend how personal data is handled in the cloud' [197]. While pointing out the problem of consumers' differential control over different layers in different service models, Hasan and Zawoad enumerated different data protective solutions such as (1) protection against exploiting co-tenancy, (2) secure architecture for the cloud, (3) Confidentiality of data, (4) Privacy in outsourced computation, (5) Access Control Mechanisms ,(6) Privacy-aware Identity Management , (7) Privacy preserving evidence collection, and (8) Privacy-aware Public Verifiability [178]. Kalia and others put forth an analysis of privacy issues concerning the cloud user by means of 'using trust model for taking effective measures in protecting the privacy of cloud users' [190]. Joshi and others mainly focussed 'on the Data Storage issues, especially on how to secure the private and confidential data of the users' [183]. Pearson stated that the 'the overarching means of addressing privacy issues in cloud computing are analysed, with a focus on privacy by design, security and accountability' [188]. ENISA reports that privacy by design was first widely presented by Ann Cavoukian and it refers 'the notion of embedding privacy measures and privacy enhancing technologies (PETs) directly into the design of information technologies and systems. Nowadays, it is regarded as a multifaceted concept: in legal documents, on one hand, it is generally described in very broad terms as a general principle; by computer scientists and engineers, on the other hand, it is often equated with the use of specific privacy enhancing technologies. However, privacy by design is neither a collection of mere general principles nor can it be reduced to the implementation of PETs. In fact, it is a process involving various technological and organizational components, which implement privacy and data protection principles' [198]. ENISA prescribed the following strategies for privacy by design in Table 21 [198]. In a recent contribution to the domain of privacy in CC Ghorbel and others extensively dealt with issues of securing privacy, mentioning both techniques of and approaches to preserving privacy in the CC environment It is shown in Table 22 **.** Indeed, there are others who also suggested solutions to safeguard data and privacy [160] [199][178] [200] [201] [202] [203][213] [214].

©IJRASET: All Rights are Reserved

However, point is that risks of data escape or loss of privacy may not necessarily disappear. Privacy problems in the cloud domain will remain, argue Shankawar and Pawar, 'for long time' and the problems may turn out to be even 'more hazardous. The issues range from malicious insiders, misuse of cloud computing and many more' [182]. Tchifilionova argues that privacy, along with security, will continue to remain problematic until the users 'become fully aware of the "depth" of the cloud: who manages it, how he does it and whether the company can afford to "give away" its information - decision that can only be taken after a careful risks analysis and policy considerations otherwise we may simply get lost in the cloud' [204]. Camenisch et al.draws attention to the widening gap between individuals' need to retain their autonomy and retain control over their personal information, irrespective of their activities', in the new information society,on the one hand, and 'current practices on electronic information networks' on the other, which is eroding individuals' trust as well as threatening critical cloud domains and democracy'. Unlike what the users did in managing normally in the traditional way is proving insufficient in the digital society for a variety of reasons. 'First, we are often not aware what data about ourselves we are revealing in a transaction or we might even not be aware of the fact that we are revealing data to start with (e.g., making a call with a mobile phone reveals all kinds of (unexpected) data to unexpected parties). Second, the sheer complexity of the applications and their building blocks makes it almost impossible to understand where our data flows. Third, even if we were capable and willing to manage our electronic personal data and identities and protect our privacy, we would usually not be able to do so because the applications don't allow us to do so due to the way they are built' [205]. This only means that technical solutions 'alone cannot protect an organization's information' and role of the human factors cannot be ignored [206]. This being the case, neither technological solutions for safe guarding data privacy nor the cyber security tools (viz, authentication, authorizatio, nonrepridation to protect confidentiality, integrity, and availability) [207] will be of much use in preventing risks from jeopardising information privacy. To cite an example: 'Companies have anonymized data sets by removing some of the data, changing the time stamps, or inserting deliberate errors into the unique ID numbers they replaced names with. It turns out, though, that these sorts of tweaks only make de-anonymization slightly harder. This is why regulation based on the concept of "personally identifying information" doesn't work. PII is usually defined as a name, unique account number, and so on, and special rules apply to it. But PII is also about the amount of data; the more information someone has about you, even anonymous information, the easier it is for her to identify you' [143]. Table 22 thus shows Technical Risks and Security Issues including Privacy in CC [208]. This Table may be compared with Table No 23, taken to show comparison of security risks in both traditional computing and cloud computing to illustrate respective advantages with data security implications especially in the cloud [**243**]. Table 23 can also be read with Table No. 15 cited earlier. But this is only one facet of the totality of the CC.

Privacy by Design Strategies		
No.	PRIVACY BY DESIGN STRATEGY	DESCRIPTION
1	Minimize	The amount of personal data should be restricted to the minimal amount possible (data minimization).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

Table 21: Privacy by Design Strategies (ENISA)

©IJRASET: All Rights are Reserved

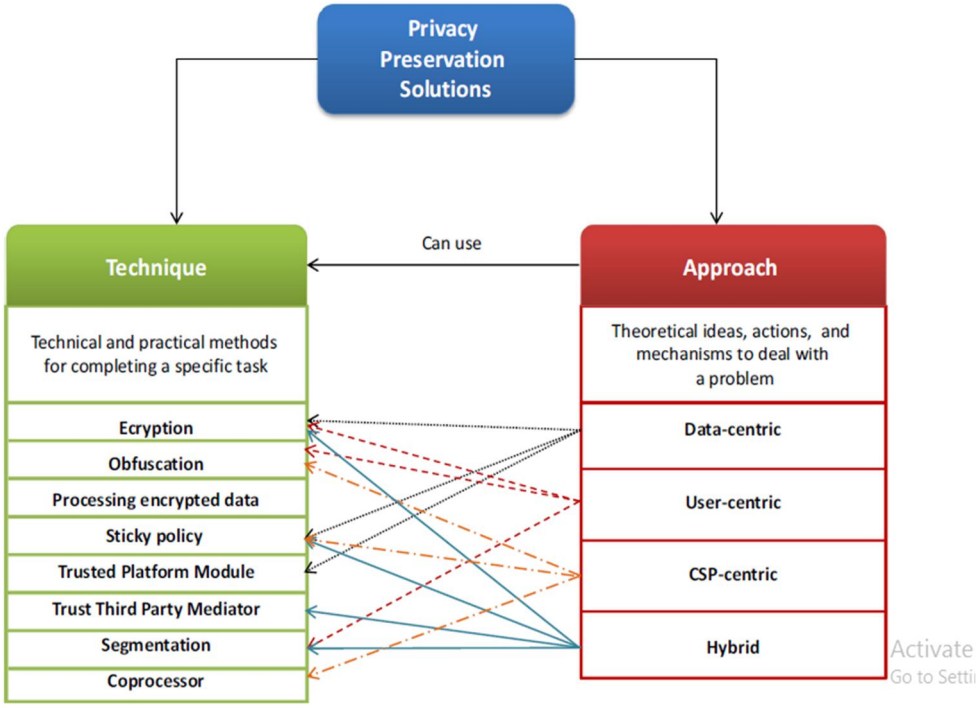


Table 22: Solutions for Privacy Protection

Risks identified	Description	Security issues
Resource exhaustion	There is a level of calculated risk in allocating all the resources of a cloud service, because resources are allocated according to statistical projections. Inaccurate modelling of resources usage-common resources allocation algorithms are vulnerable to distortions of fairness or inadequate resource provisioning and inadequate investments in infrastructure can lead, from the Cloud Provider (CP) perspective, to: Service unavailability, access control compromised, economic and reputational losses and infrastructure oversize	Availability, Integrity, Privacy, Accountability
Isolation failure	This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure	Availability, Integrity, Privacy, Accountability
Cloud provider malicious insider	The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. This can be considered especially important in the case of cloud computing due to the fact that cloud architectures necessitate certain roles which are extremely high risk	Integrity, Privacy, Accountability
Management interface compromise	The customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities	Integrity, Privacy, Accountability

©IJRASET: All Rights are Reserved

Intercepting data in transit	Cloud computing, being a distributed architecture, implies more data in transit than traditional infrastructures. Sniffing, spoofing, man-in-the-middle attacks, side channel and replay attacks should be considered as possible threat sources	Integrity, Privacy
Data leakage on up/download, intra-cloud	It's the same previous risk considered between cloud provider and cloud customer	Integrity, Privacy
Insecure or ineffective deletion of data	Whenever a provider is changed, resources are scaled down; physical hardware is reallocated, etc. Data may be available beyond the lifetime specified in the security policy. It may be impossible to carry out the procedures specified by the security policy, since full data deletion is only possible by destroying a disk which also stores data from other clients	Integrity, Privacy
Distributed denial of services (DDoS)	Is an attempt to make a machine or network resource unavailable to its intended users	Availability
Economic denial of service	There are several different scenarios in which a cloud customer's resources may be used by other parties in a malicious way that has an economic impact: Identity theft, payments, loans, etc.	Availability
Loss of encryption keys	This includes disclosure of secret keys (SSL, file encryption, customer private keys, etc.) or passwords to malicious parties, the loss or corruption of those keys, or their unauthorized use for authentication and non-repudiation (digital signature)	Integrity, Availability, Privacy
Undertaking malicious probes or scans	Malicious probes or scanning, as well as network mapping, are indirect threats to the assets being considered. They can be used to collect information in the context of a hacking attempt	Availability, Integrity, Privacy
Compromise service engine	Hacking the service engine may be useful to escape the isolation between different customer environments (jailbreak) and gain access to the data contained inside them, to monitor and modify the information inside them in atransparent way (without direct interaction with the application inside the customer environment), or to reduce the resources assigned to them, causing a denial of service	Availability, Integrity, Privacy, Accountability
Conflicts between customer hardening procedures and cloud environment	Cloud providers must set out a clear segregation of responsibilities that articulatesthe minimum actions customers must undertake. The failure of customers to properly secure their environments may pose a vulnerability to the cloud platform if the cloud provider has not taken the necessary steps to provide isolation. Cloud Providers should further articulate their isolation mechanisms and provide best practice guidelines to assist customers to secure their resources	Integrity, Privacy

Table 23:Cloud Computing: Technical Risks and Security Issues including Privacy

©IJRASET: All Rights are Reserved

Principal characteristics		Advantages		Data security implications in the cloud
Cloud infrastructure	Traditional infrastructure	Cloud infrastructure	Traditional infrastructure	
Leased infrastructure	Proprietary infrastructure	Cost reduction abstraction of hardware and software management constraints, physical security	Better control over infrastructure, more cost-effective when needs are "stable"	Loss of control over data ->risks related to data confidentiality, integrity and availability
Open infrastructure	Closed infrastructure	High availability	Better security level	Unauthorized access ->Risks related to data confidentiality, integrity and availability
Shared infrastructure	Dedicate infrastructure	Cost reduction-collaboration between users optimized management of physical infrastructure	Physical isolation between users	Unauthorized access between Cloud consumers ->Risks related to data confidentiality, integrity and availability
Elastic infrastructure (scale up/down)	Rigid infrastructure (scale up)	Cost reduction-resources using optimization	Simpler infrastructure management	Risks related to data confidentiality (resource reuse, case of data remanence)
Multi-level Virtualization (infrastructure, platform, application)	Virtualization possible, usually on a single level	Cost reduction-optimization and easier maintenance of physical resources flexibility-simple, fast and dynamic management of virtual resources	Easier infrastructure management better security	Classical virtualization risks (hypervisor, virtual machines, virtual network, and the problem of sharing physical resources) ->Risks on data confidentiality, integrity and availability
Distributed infrastructure	Centralized infrastructure	High availability, better fault tolerance	Easier, more controlled and more secure infrastructure management	High risk on data confidentiality and privacy but also on integrity

Table 23: Data security implications according to Cloud characteristics compared to traditional infrastructure

The other facet is the risks associated with the rise of the information/knowledge/digital society in which mainly the entire facet of the totality of the CC -- the computer and internet-- the ICTs in brief --play a universalizing role and create 'a sea change in today's life' [209] . Stated otherwise, it impacted all conceivable aspects society and everyday life of the individual. The rise of computers and internet from the 1960s and 1970s coincided with the appearance of information society, rather information risk society pervaded by 'digitisation and datafication', which opened the doors to 'possibilities for monitoring, profiling and tracking presence and behaviour' of the people in the '40-billion-dollar global data market' [210]. The issue of the information privacy as a risk come into sight in view of the fact that 'the introduction in the 1960s of sophisticated information technology systems that enabled the automated processing of information led to a re-evaluation of the privacy right and to a claim that the protection of privacy should extend to information collected and processed by such systems. Those systems' ability to store and categorise information, link it to other information and make that information easily accessible to users led to fears that they could be used in ways that inhibited individuals' ability to control the use of their personal information by both public and private organisations' [211]. As far back as 1964 Packard, in his The *Naked Society*, apprehended that, much before the arrival computer and internet, 'privacy is becoming harder and harder to attain, surveillance more and more pervasive' [212]. But their arrival changed the entire scenario, transforming erstwhile society into information/knowledge/ digital society and, simultaneously embedding risks therein.

©IJRASET: All Rights are Reserved

The arrival of the computers in the 1970s were seen as 'some sort of magical calculating engine 'or 'the experimental toys of university researchers'. But soon, with the emergence of powerful, cheap, mass - produced computers-on-a-chip', computers -- machines for 'the automatic processing o f *information*'-- to rose to position of a giant computer industry changing the way people lived their lives by virtue of the 'productivity and social enhancements' it brought about and now tiny computers - pocket calculators, cameras , etc-can be seen everywhere [215][216]. It is no truism to agree with Berry: 'Computers are entangled with our lives in a multitude of different, contradictory and complex ways, providing us with a social milieu that allows us to live in a society that increasingly depends on information and knowledge. More accurately, we might describe it as a society that is more dependent on the computation of information, a *computational knowledge* society' [217].

Challenging Aspects of Computer Security		
1	intelligent, adaptive adversary	while most science relies on nature not being capricious, computer security faces an intelligent, active adversary who learns and adapts, and is often economically motivated.
2	no rulebook	attackers are not bound to any rules of play, while defenders typically follow protocol conventions, interface specifications, standards and customs.
3	defender-attacker asymmetry	attackers need find only one weak link to exploit, while defenders must defend all possible attack points.
4	scale of attack	the Internet enables attacks of great scale at little cost—electronic communications are easily reproduced and amplified, with increasing bandwidth and computing power over time.
5	universal connectivity	growing numbers of Internet devices with any-to-any packet transmission abet geographically distant attackers (via low traceability/physical risk).
6	pace of technology evolution	rapid technical innovation means continuous churn in hardware devices and software systems, continuous software upgrades and patches.
7	software complexity	the size and complexity of modern software platforms continuously grows, as does a vast universe of application software. Software flaws may also grow in number more than linearly with number of lines of code.
8	developer training and tools	many software developers have little or no security training; automated tools to improve software security are difficult to build and use.
9	interoperability and backwards compatibility	interoperability requirements across diverse hardware-software and legacy systems delays and complicates deploying security upgrades, resulting in ongoing vulnerabilities even if updates are available.
10	market economics and stakeholders	market forces often hinder allocations that improve security, e.g., stakeholders in a position to improve security, or who would bear the cost of deploying improvements, may not be those who would gain benefit.
11	features beat security	while it is well accepted that complexity is the enemy of security, little market exists for simpler products with reduced functionality.
12	low cost beats quality	low-cost low-security wins in "market for lemons" scenarios where to buyers, high-quality software is indistinguishable from low (other than costing more); and when software sold has no liability for consequential damages.
13	missing context of danger and losses	cyberspace lacks real-world context cues and danger signals to guide user behavior, and consequences of security breaches are often not immediately visible nor linkable to the cause (i.e., the breach itself).
14	managing secrets is difficult	core security mechanisms often rely on secrets (e.g., crypto keys and passwords), whose proper management is notoriously difficult and costly, due to the nature of software systems and human factors.
15	user non-compliance (human factors)	users bypass or undermine computer security mechanisms that impose inconveniences without visible direct benefits (in contrast: physical door locks are also inconvenient, but benefits are understood).
16	error-inducing design (human factors)	it is hard to design security mechanisms whose interfaces are intuitive to learn, distinguishable from interfaces presented by attackers, induce the desired human actions, and resist social engineering.
17	non-expert users (human factors)	whereas users of early computers were technical experts or given specialized training under enterprise policies, today many are non-experts without formal training or any technical computer background.
18	security not designed in	security was not an original design goal of the Internet or computers in general, and retro-fitting it as an add-on feature is costly and often impossible without major redesign.
19	introducing new exposures	the deployment of a protection mechanism may itself introduce new vulnerabilities or attack vectors.
20	government obstacles	government desire for access to data and communications (e.g., to monitor criminals, or spy on citizens and other countries), and resulting policies, hinders sound protection practices such as strong encryption by default.

Table 24: Challenges of computer Security

©IJRASET: All Rights are Reserved

In view of the fact that 'data revolution' is giving rise to 'datafied' information society or a digital society experiencing 'datamization' and exhibiting what is called 'data love', the role of the computer becomes notably important in the matter of data or information privacy. The explosive growth of networked computers in 'gathering data, creating data, storing data, and analyzing data' is conducive to the generating a space that is invasive of privacy and generative of 'computer crime' [139][145] [136] [140] [218]. Table 24 above shows the various challenging aspects of computer security, pointing to the threats and risks that may translate into computer crime [219]. Payton and Claypoole states that information has become 'king' and 'the deeper technology becomes embedded into our lives, the more it threatens our privacy' [136]. A UK government 1975 White Paper listed a number of reasons about how computers erode privacy resulting in the production of privacy risks. 'First, they facilitate the maintenance of extensive records systems and the retention of data. Such records tend to grow 'out of control', and organizations collect more data than is necessary for the original task. Second, computers make data easily and quickly available from many different points, which make possible unauthorized access to information, its theft or alteration. Third, data can be transferred from one information system to another, making possible the compilation of centralized dossiers on individuals and the resale of private information. Data can be combined to give new information using powerful relational databases which make the merging of records cost-effective. Finally data is in machine-readable form which means that few people may know of the data or the uses to which it is put' [220]. A keen observer of the workings of computer, Schneier has this to say: 'The pervasiveness of computers has resulted in the almost constant surveillance of everyone, with profound implications for our society and our freedoms. Corporations and the police are both using this new trove of surveillance data. ... The common thread here is computers. Computers are involved more and more in our transactions, and data are byproducts of these transactions. As computer memory becomes cheaper, more and more of these electronic footprints are being saved. And as processing becomes cheaper, more and more of it is being cross-indexed and correlated, and then used for secondary purposes'[252]. No wonder, cybersecurity issues are becoming 'a day-to-day struggle' for business organizations. Most companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss. 68% of business leaders feel their cybersecurity risks are increasing. Hackers attack every 29 seconds, on average 2,244 times a day. 500 million consumers, dating back to 2014, had their information compromised in the Marriott-Starwood data breach made public in 2018. Data breaches exposed 4.1 billion records in the first half of 2019. 71% of breaches were financially motivated and 25% were motivated by espionage. 52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively. Security breaches have increased by 11% since 2018 and 67% since 2014. 34% of data breaches involved internal actors. 71% of breaches were financially motivated and 25% were motivated by espionage. On average, every employee had access to 17 million files. The average time to identify a breach in 2019 was 206 days. Financial and Manufacturing services have the highest percent of exposed sensitive files at 21%. The financial services industry takes in the highest cost from cybercrime at an average of $18.3 million per company surveyed. The banking industry incurred the most cybercrime costs in 2018 at $18.3 million [221]. However, there have been attempts to address the most 'common computer security' problems and their solutions, not specifically privacy erosion [222]. Against this backdrop, it is understandable why someone could say that 'The only safe computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location' [206]. The year 1981 is pivotal from the perspective of computer crime when first arrest was made for hacking into A&T Systems to change the systems' internal clocks. The 1980s witnessed the growth of computer crime but the decade of 1990s marked a transition for computer crime due to the availability of the needed skills to break into the computer along with increasing accessibility of internet. By the early part of the 21 first centuries organized crime took significant control of the cyber world. Now, more than ever before, 'the Internet has become a hotbed oforganized criminalactivities and criminal groups are using cyberspace in every way conceivable' [223]. Internet is 'the electronic network of networks that links people and information through computers and other digital devices allowing person-to person communication and information retrieval' [224]. Cyberspace basically consists of 'consists of hardware, operating systems, communication networks, and applications.There is a supplementary layer composed of the frameworks that allow the execution of applications' [225]. The Information Age is witnessing Big Data, 'Supercomputing at Internet scale', now being dealt with by such companies as Google, Facebook, Yahoo and others, in view of the need 'to process the ever-increasing numbers of users and their data which was of very large volume, with large variety, high veracity and changing with high velocity which had a great value' [226]. Since the scope of Big Data is extremely wide, 'Big Data can also lead to big problems'. For instance, the revelation of NSA meta-data collection is marked by such implications concerning the future counterterrorism and also public trust in the government. The case Netflix also exhibits danger of Big Data for privacy. 'After releasing a de-identified list of user movie preferences to crowd-source an improvement to their recommendation algorithm, executives were shocked to learn that researchers could tie this data to real identities. In one instance, a list of what movies someone liked was enough to determine his or her closeted sexual orientation. More data, and better tools to understand it, can yield unprecedented knowledge, but they may also break down human

©IJRASET: All Rights are Reserved

social, legal, and ethical boundaries we aren't yet ready to cross' [227]. Edward Snowden's revelations of highly classified information of the National Security Agency (NSA) clearly demonstrate the failure of the domestic and international legal infrastructure to keep pace with technological advancements. 'The USA PATRIOT Act and other national security laws were ill-equipped to handle developments in bulk data collection' [228]. There is no need to emphasize the benefits and efficacy of the internet – a transformative technology- which is 'ubiquitous in everyday life and it is here obviously to stay' in view of its impacts on the society and as part of daily lives as transformative technology [224] [229] [230] [231]. But, relevant to the objective of the present paper, there is also a flip side to the internet. And this about risks embedded in the internet. In addition to collecting, assembling, and storing data by both corporation and states for profit and security, internet of things now stand for 'connected devices generate enormous volumes of data about our movements, locations, activities, interests, encounters, and private and public relationships through which we become data subjects. When joined up with other data collected by private or public authorities concerning our taxes, health,passport, travel, and finance, the data profiles that can be compiled about people is staggering ... Some of the Internet's novel aspects, such as the speed and reach of interactions and transactions, have spurred concerns about high-frequency trading, the hacking of financial and banking services, state and corporate spying on citizens, deliberate cross-border virus attacks, covert cyberwars among states, and the rise of often anonymous racism, xenophobia, and homophobia along with cyberbullying and issues of freedom of speech' [105]. In order to prevent data privacy businesses often anonymize the PII of the customer but the point is that PII is also about a quantity of data and 'the more information someone has about you, even anonymous information, the easier it is for her to identify you'. Again, the internet companies such as Facebook and Google improved their product offerings to their actualcustomers by 'reducing user privacy' by changing policies or defaultsettings respectively [143]. Moreover, as Snowdens' revelations make clear, the through programs like PRISM, the NSA legally compels internet companies like Microsoft, Google, Apple, and Yahoo to provide data ofcitizens of its own interest. Thereare other programs that enable the NSA to get 'direct access to the Internetbackbone to conduct mass surveillance on everyone'. Sometimes those corporations cooperate and sometimes they are forced. What is even more interesting that the NSA itself hacks into the infrastructure of those corporations without their consent. 'This is happening all over the world. Many countries use corporate surveillance capabilities to monitor their own citizens. ...The net result is that a lot of surveillance data moves back and forth between government and corporations. One consequence of this is that it's hard to get effective laws passed to curb corporate surveillance—governments don't really want to limit their own access to data by crippling the corporate hand that feeds them' [143]. Ghernaouti, in an ITU document, points to 'the fragility of confidence' in data privacy in view of the new cyber threats and risks confronting cyberspace. 'These are still far too often insufficiently recognised and misunderstood and thus easily create fear. We cannot necessarily predict when or how these threats will become reality, or the domino effects and sequences of events they will provoke, or identify their authors and the people behind them. As a result most notably of the WikiLeaks (2010) and Prism (2013) affairs, we now know for certain that digital secrecy does not exist and that we are kept on a close electronic leash and tracked, followed, observed and monitored' [232]. Widespread use of internet electronic commerce, for instance, has many implications such as for 'intellectual property rights, privacy protection, and data filtering, etc.' affecting both organization and society and often producing social concerns and adverse consequence for the digital economy driven by the ICTs [233] [97]. To sum up,'in the digital age, privacy is considered in a new context. It is no more confined to protection of the physical and material environment, such as the home, mail or documents, but now extends to the huge volume of personal data in cyberspace, and to the high level of connectivity that is turning each individual into a "sensor for the world intelligence community". There is no global consensus on what can be considered as adequate protection of privacy' [232]. There is little doubt that invasion of privacy on the internet is 'a significant issue' in the information age [234].

VII. CONCLUDING REMARKS

The foregoing analysis leads to finding that the Information/knowledge/ digital society is becoming, if it has not already become, a 'surveillant society' [235-240] in view of its inherent privacy concerns and associated risks because of its embodiment of digital technologies especially in the computer and internet. There is not great firewall to ensure complete privacy for the individual, organizations or the national state. Ironically, they are also involved in the privacy invasive practices for their interests and profits in the digital IS. The new surveillance is 'the use of technical means to extract or create personal data. This is may be taken from individuals or contexts' [241]. As a matter of fact, researchers undertaking studies in computer surveillance in the IS have coined different terms for encompassing darker dimensions including privacy erosion, such as 'dataveillance, the electronic (super) panopticon, electronic surveillance, or digital surveillance' [242]. It is however to be noted that surveillance has two sides: benefits, on the one hand, and problems and risks, on the other. While benefits such as 'correct identification, screening, checking,

©IJRASET: All Rights are Reserved

appropriate classificationand other tasks associated with it must be acknowledged', one should also should not be oblivious of its 'dangers and risks'. In Beck's words they represent the 'bads' [239]. In the wake of the Third and Fourth Industrial Revolutions, the IS has basically emerged as Information Risk Society. Pinter who catalogues numerous social risks (viz. 'exploitation of workers (especially children, women, minority and elderly employees), destruction of jobs (high unemployment rates), environmental pollution, threatening of privacy and freedom, increasing xenophobia and intolerance, dividing the society, end of solidarity, increasing poverty and inequality') came to the conclusion that in the late modern society 'we are at the beginning of a new era, which is an information risk society' [244]. In view of the vulnerabilities (viz. Paradigmatic risks, Risks from inadequate implementation, Risks from usage, Risks from deliberate misuse) in the computer system, the users experience risks , and hence Brunnstein points to the emergence of ' the Information/Knowledge society as Risk Society' [245].

The concept of Risk Society (RS) is a new paradigm introduced by Beck to conceptualize the nature and character of the society late modernity of the contemporary industrial society. He writes that 'the risk society is thus not a revolutionary society, but more than that, a *catastrophic society*. In it the *state of emergency* threatens to *become the normal state*' [246]. For Beck, the risk society is a kind of society that systematically produces, defines and distributes 'techno-scientifically produced risks'. Accordingly, (risk) problems and conflicts in such a society arise 'from the production, definition and distribution of techno-scientifically produced risks' [246]. 'The transition from the industrial to the risk epoch of modernity occurs *un*intentionally, *un*seen, compulsively, in the course of a dynamic of modernization which has made itself autonomous, on the pattern of *latent side-effects* … Risk society is *not an option* which could be chosen or rejected in the course of political debate. It arises through the automatic operation of autonomous modernization processes which are blind and deaf to consequences and dangers' [247]. The risk discourse is concerned with techno-scientifically produced 'bads' (viz. radiation). They are uncontrollable and their consequences are incalculable and hence 'cannot be insured against' [248]. The RS appears at the very moment when the hazards – the 'bads'—begin to '*undermine and/or cancel the established safety systems*' and defy 'existing risk calculation ', eventually mutating 'into risk society through its own systematically produced hazards, balances *beyond the insurance limit*' [249]. If information/knowledge/digital society has emerged as surveillant risk society, CC has also emerged as a computing risk environment, as has been analysed in the present paper with the primary objective of illustrating privacy risks. In the first and last instances CC, along with security and privacy issues and concerns, is embedded in the IS. Privacy risks are built into the CC environment that provides the platform of both computer and internet, the uses of both of which have almost become widespread in varying degrees across the world via the process of globalization. The truth of the matter is that both CC and globalization reciprocally feed and accelerate each other. While information/surveillant risk society is expanding, similarly privacy risks has increasingly come into view as one of most difficult security issues according to most analysts even if CC is in the process of a larger scale of adoption by individuals, organization and even the nation – states. This is in spite of inherent problem of privacy and security risks associated with the CC. A *Report* of the ITU on the CC privacy rightly points out that 'without knowledge of the physical location of the server or of how the processing of personal data is configured, end-users consume cloud services without any information about the processes involved. Data in the cloud are easier to manipulate, but also easier to lose control of. For instance, storing personal data on a server somewhere in cyberspace could pose a major threat to individual privacy. Cloud computing thus raises a number of privacy and security questions. Can cloud providers be trusted? Are cloud servers reliable enough? What happens if data get lost? What about privacy and lock-in? Will switching to another cloud be difficult? ... Privacy issues are increasingly important in the online world. It is generally accepted that due consideration of privacy issues promotes user confidence and economic development. However, the secure release, management and control of personal information into the cloud represent a huge challenge for all stakeholders, involving pressures both legal and commercial. .. Cybercriminal activities impacting cloud computing environments -- for example, fraud and malicious hacking -- are threats that can undermine user confidence in the cloud. Cloud computing providers face multiple, and potentially conflicting, laws concerning disclosure of information. Achieving a better understanding of jurisdictional issues is critical and should be tackled through enhanced dialogue' [250]. As Ghernaouti puts it succinctly, 'cyber-risks are a reality for everyone' [232]. In the light my analysis and survey on the risks accompanying both CC and RS, it is needless to elaborate any further how both are analogous. Both are essentially an outcome of techno-scientific origin and involved human factors. Both are global in nature and occur in the global information capitalist market in the networked informational society. Last but not the least, both are involved in or subject to concerns such as threats, attacks, vulnerabilities, trusts, data privacy and surveillance within national and international boundaries. As far privacy issues are concerned, it will be in the fitness of things to conclude, despite many positive efforts including privacy-enhancing technologies (PETs), in the borrowed words of with Aspinall et al. about the risks and issues of ensuring privacy: 'privacy remains highly vulnerable. Rapid technology developments and increasing interest in identities and other personal data from commercial and government sectors have fuelled increasing data collection to privacy's

©IJRASET: All Rights are Reserved

detriment, with little apparent financial advantage in its protection. Laws and regulation have been faltering for various reasons: weak and slow implementation, ineffective sanctions, and easy circumvention. Many laws aim at checkbox compliance rather than promoting the actual protection of human rights. Technology and processes have become so complex that not even experts – let alone end-users – can tell whether or not privacy is being protected; hence protective measures are inhibited. This makes it more difficult for user-controlled identity management to succeed in empowering users. Moreover, the Snowden revelations in 2013 made it clear that electronic infrastructures are very vulnerable, and protection mechanisms such as encryption are rarely used. Identity information of Internet and phone users is being collected and analyzed by intelligence services in the pursuit of national security. This is problematic not only for maintaining privacy and managing one's identities, but for the organization and structure of societies and economies in general' [251].

VIII. ACKNOWLEDGEMENT

The author gratefully acknowledges all the support and encouragement received from Bipul Kumar Bhadra, PhD (McMaster), a former Professor of Jadavpur University, Kolkata, West Bengal, India.

REFERENCES

[1] ITU,(International Telecommunication Union). 2017. *Measuring the Information Society Report*, vol. 1, Geneva: Switzerland, 2017, pp 105, 107.
[2] W. Genovese, "Accelerating success in the 4th industrial revolution", https://www.huawei.com/uk/about-huawei/publications/winwin-magazine/29/accelerating-success-in-the-4th-industrial-revolution, 2017.
[3] S. Klus,*The Fourth Industrial Revolution*. Geneva: World Economic Forum, 2016, p.7.
[4] Kumar, K. et al., Industry*4.0. Developments towards the Fourth Industrial Revolution*. Singapore: Springer, 2019 pp. v-vi.
[5] Aissam, M. et al."Cloud Robotic: Opening a New Road to the Industry 4.0", in N. Debel et al. (eds.): *New Development and Advances in Robot Control* Singapore: Springer**,** 2018, pp. 1-20.
[6] M. J. Kavis, *Architecting The Cloud: Design Decisions for Cloud Computing Models (SaaS, PaaS, and IaaS). Wiley*,2014, p. 34.
[7] S. Murugesan and I. Bojanova. "Cloud Computing: An Overview", IEE Computer Society: Wiley, in (eds.) San Murugesan and I. Bojnana, *Encyclopaedia of Cloud Computing*, *IEE Computer Society*, Wiley, 2016, pp. 4, 10-11.
[8] B. Sosinsky. 2011. *Cloud Computing Bible*, Wiley: Indianapolis, 2011.
[9] Arif Mohamed, "A history of cloud computing", *Computer Weekly. Com.* Retrieved from https://www.2roads.com/2010/08/13/a-history-of-cloud-computing/, 2010
[10] M. Bohm et al., "Cloud Computing and Computing Evolution", Retrieved from*https://www.researchgate.net/publication/268011245*,2014 *p.9.*
[11] P.S. Deshpande et al. 2019. *Security and Data Storage Aspect in Cloud Computing*, Springer: Singapore, p. 2-4.
[12] S. Bhowmik, *Cloud Computing*, Cambridge: Cambridge University, 2017, pp. 31, 69, 206.297.
[13] R. Buyya et al., *Mastering Cloud Computing Foundations andApplications Programming*, Elsevier: Amsterdam,2013, pp.7-9.
[14] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing", *Electrical Engineering and Computer Sciences: University of California at Berkeley*,2009, p.4.
[15] NIST(National Institute of Standards and Technology). NIST Special Publication 800-145**,** *October 25, 2011***.** *Final Version of NIST Cloud Computing Definition Published*, P. Mell and T. Grance, NIST: Gaithersburg, MD, 2011, P. 2.
[16] L. Chen, et al. (eds.), *Security, privacy, and digital forensics in the cloud*, Singapore: Wiley, 2019, p. 4.
[17] NIST (National Institute of Standards and Technology- NIST Special Publication 500-292). 2011. (eds. F. Liu et al., *NIST Cloud Computing Reference Architecture*, NIST: Gaithersburg, MD, 2011,pp. 3-4.
[18] P. Ugyel, A *Cloud Computing Training Platform*. Unpublished Dissertation: Bharathidasan University, 2002, pp. 15-6
[19] S. Chhabra and V.S. Dixit, "Cloud Computing: State of the Art and Security Issues," *ACM SIGSOFT Software Engineering Notes*, 30(March), 2015, pp.. 1-2.
[20] S.P.Chandran and M. Angepat 2010. "Cloud Computing: Analysing the Risks involved in Cloud Computing Environments", Retrieved from *https://www.semanticscholar.org*, 2010, pp. 1-2.
[21] DataFlair Team, . "Features of Cloud Computing – 10 Major Characteristics of Cloud Computing", https://data-flair.training/blogs/features-of-cloud-computing/, 2019
[22] C.T.S. Xue and F.T.W. Xin, "Benefits and Challenges of the Adoption of Cloud Computing in Business", *International Journal of Cloud Computing Services and Architecture*, 2016, vol. 6 (6), pp.3-7.
[23] M.M. Alan, *Elements of Cloud Computing Security: a Survey of Key Practicalities*, Springer: Switzerland, 2017,pp. 12-3.
[24] S. Srinivasan, *Cloud Computing Basics*, Springer: New York, 2014, p. 107.
[25] M.T. Amron et al., "A Review on Cloud Computing Acceptance Factors", *Procedia Computer Science*, 124, 2017, pp. 640,643-4.
[26] K. Hashizume, et al., "An Analysis of Security Issues for Cloud Computing", *Journal of Internet Services and Applications*, 2013, 4(5), pp. 1-2.
[27] G. Garsson et al., "Success Factors for Deploying Cloud Computing',*Communications of The ACM*, DOI:10.1145/2330667.2330685,2012, 55(9), pp. 63, 66.
[28] F.N. Njeh, *Cloud Computing: An Evaluation of the Cloud Computing Adoption and Use Model*, Unpublished PhD dissertation. Bowie, MD: Bowie State University, 2014, p. 15.
[29] J. Zelenay et al., "Cloud Technologies – Solutions for Secure Communication and Collaboration", Procedia Computer Science, 15, 2019, p. 568.
[30] NIST (Special Publication 500-291, Version 2), *NIST Cloud Computing Standards Roadmap*, http:/dx.doi.org/10/6028/NIST.SP.500-291r2, 2013, pp. 9-10.

©IJRASET: All Rights are Reserved

[31] H.B. Rebah and H. B. Sta, "Cloud Computing: Potential Risks and Security Approaches", in (eds.), T.F. Bissyande and O. Sie, *e-Infrastructure and e-Services for Developing Countries*, Springer: Switzerland, 2018, p.72.
[32] D.A.B. Fernandes et al., "Security Issues in Cloud Computing Environments: A Survey", *International Journal of Information Security*, 13, 2014, p.121.
[33] UN (United Nations), *Managing cloud computing services in the United Nations system*, United Nations • Geneva, 2019, p. 1..
[34] M. Castells, *The Rise of the Network Society: The Information Age*, vol. 1, Wiley-: Blackwell: Sussex, UK, 2010, p. 5.
[35] M. Castells, *The Rise of the Network Society: End of Millennium*, vol. III, Blackwell: Sussex, UK, 2010, p. 372.
[36] OIIP (Office of International Information Programs)..*Okinawa Charter of Global Information Society*. Available at https://www.mofa.go.jp/policy/economy/summit/2000/documents/index.html Accessed on 10 May 2000, paras 2-3.
[37] EU (European Union). . "Presidency Conclusions: Lisbon European Council 23 and 24 March 2000", Available at http://www.euroskop.cz/files/19/E20B93F3-53EA-4A95-84EF-AC6995553DB9.pdf, Accessed on 23 April 2020.
[38] EC (European Commission),*Third European Report on Science & Technology Indicators: Towards a knowledge-based economy*. Luxembourg: Office for Official Publications of the European Communities, 2003, p. 38.
[39] NASSCOM, Cloud: Next Wave of Growth in India, NASSCOM: Noida, New Delhi, 2019, p.13.
[40] C. J. Hamelink, "New Information and Communication Technologies, Social Development and Cultural Change" UNRISD (United Nations Research Institute for Social Development): Geneva, Switzerland, 1997, pp. 3-4
[41] A. Danielewicz-Betz, *Communicating in Digital Age Corporations*, Palgrave Macmillan: London, 2016, pp. 23-4
[42] N. Urbachand F. Ahlemann, *IT Management in the Digital Age*, Springer: Switzerland, 2019, p. 3.
[43] Gartner, "Information Technology, Gartner Glossary : Digital", https://www.gartner.com/en/information-technology/glossary/digital-2, Accessed on 12 January 2020.
[44] Gartner, "Information Technology, Gartner Glossary : Digitalization", https://www.gartner.com/en/information-technology/glossary/digitalization, Accessed on12 January 2020.
[45] TruQC, "Digitization vs. digitalization: Differences, definitions and examples", https://www.truqcapp.com/digitization-vs-digitalization-differences-definitions-and-examples/
[46] N. Urbach and M. Röglinger, "Introduction to Digitalization Cases: How Organizations Rethink Their Business for the Digital Age", in (eds.), *Digitalization Cases: How Organizations Rethink Their Business for the Digital Age*, Springer: Switzerland, 2019, pp. 1-3.
[47] N. Urbach and F..Ahlemann, *IT Management in the Digital Age: A Roadmap for the IT Department of the Future*, Springer: Switzerland, 2019, p. 3.
[48] R. Silberglitt et al., *The Global Technology Revolution 2020, In-Depth Analyses*, RAND Corporation, Santa Monica, California, 2006, p.xvii.
[49] I. Miles, "Contemporary Technological Revolutions: Characteristics and Dynamics", in (ed.) M. R. Bhagvan, *New Generic Technologies in Developing Countries*, London: Macmillan, 1997, PP. 25-42.
[50] ITU, *WSIS-Geneva Declaration of Principles*, https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1161%7C1160.
[51]] ITU, WSIS--*Report of the Tunis phase of the World Summit on the Information Society 2005*, https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=2331|2304
[52] Government of India, National Knowledge Commission Report to the Nation 2006-2009, https://www.aicte-india.org/reports/overview/Knowledge-Commission-Report, p. 3.
[53] Martin Bangemann, *"Europe and the global information society- Bangemann report:Recommendations to the European Council*", https://www.cyber-rights.org/documents/bangemann.htm,
[54] A. Becla, "Information Society and Knowledge-Based Economy—Development Level and the Main Barriers –Some Remarks", *Economics & Sociology*, 5(1), p. 126.
[55] R. Lane, "The Decline of Politics and Ideology in a Knowledgeable Society", *American Sociological Review*, 1966, 31(5), p. 649.
[56] Z. Brzezinski, "America in the Technetronic Age", *Childhood Education*, 1968, 45:1, p. 6.
[57] S. Etzioni, *The Active Society: A Theory of Societal and Political Processes*, The Free Press: New York, 1968, pp. viii, 6.
[58] P. Drucker, *Post-Capitaslist society*, Butterworth-Heinemann: Oxford, 1993, pp. 5-7.
[59] S. Nora and A. Minc, *The Computerization of Society: A Report to the President of France*, The MIT Press: Cambridge, 1980, p. 137.
[60] A. Touraine, *The Post-Industrial Society*, Random House: New York, 1971, p.3
[61] D. Bell, "The Social Framework of the Information Society', in (ed.) T. Forester, *The Microelectronics Revolution*, The MIT Press: Cambridge, pp.500-501.
[62] D. Bell, *The Coming of Post- Industrial Society: A Venture in Social Forecasting, Special Anniversary Edition*, Basic Books: New York, 1999.
[63] D. Bell, *The Coming of Post-Industrial Society. A Venture in Social Forecasting*. New York: Basic Books, 1979.
[64] F. Webster, *Theories of the Information Society*, Routledge: London, pp. 32-59.
[65] K. Kumar, *From Post-Industrial to Post-Modern Society*, Blackwell: Oxford, 2005, pp. 29-60
[66] D. Lyon, "The Roots of the Information Society Idea', in (eds.) N. Heap et al., *Information Technology and Society*, Sage: London, 1995, pp. 54-73.
[67] J. L. Salvaggio (ed.), *The Information Society: Economic, Social and Structural Issues*, Larence Erlbaum Associates: New Jersey, 1989, pp.1-14, 29-50.
[68] Alistair S Duff, "Information Society", in (ed.), J. Wright, *International Encyclopedia of Social & Behavioral Sciences*, Elsevier: Amsterdam, 2015, vol. 12, pp. 83-9.
[69] J. B. Rule *and Y.* Besen, "The once and future information society", *Theory and Society*, 37(4), pp. 317–342
[70] M. Ampuja and J. Koivisto, "From 'Post-Industrial' to 'Network Society' and Beyond: The Political Conjunctures and Current Crisis of Information Society Theory", *tripleC*, 12(2), 2014, pp. 447-463.
[71] P. Sasvari, *The development of information and communication technology: An empirical study*, University of Miskolc, Faculty of Economics,Hungary, 2010, p. 23.
[72] Christopher T.Marsden, "Introduction: information and communications technologies, globalisation and regulation', in (ed.), Christopher T.Marsden, *Regulating the Global Information Society*, Rutledge: London, 2000, p. 1.
[73] J. A.G.M. van Dijk, *The Network Society*, Sage: London, 2006, p. 19.
[74] R. Mansell and W. E. Steinmueller, *Mobilizing the Information Society: Strategies for Growth and Opportunity*, OUP: Oxford, 2002, p. 8.

©IJRASET: All Rights are Reserved

[75] Gustav Cardoso, *The Media in the Network Society: Browsing, News, Filters and Citizenship*, Lisboa, Portugal: CIES – Centre for Research and Studies in Sociology, 2006, p.45.
[76] H.S. Dordick and G. Wang, The *Information Society*, Sage: London, 1993, p. 128.
[77] J. Feather, *The Information Society*, Facet Publishing: London, 2008, P. 201.
[78] D. Bell et al. (eds.), *Cyberculture: The Key Concepts*, Routledge: London, pp. 94-5.
[79] D.Lyon, *The Information Society: Issues and Illusions*, Polity Press: Cambridge, 1988]pp. 17-21.
[80] P. Virilio, *The Information Bomb*, Verso: London, 2005, pp. 108-12.
[81] D. Schiller, Schiller, Digital *Capitalism: Networking the Global Market System*, Cambridge, Mass.: MIT Press, 1999.
[82] R. Hassan, *The Information Society*, Polity: Cambridge, 2008, p. 27.
[83] A. S. Targowski, "The Taxonomy of Information Societies", in (ed.), Yi-chen Lan , *Global information society : Operating Information Systems in a Dynamic Global Business Environment*, Idea Group Publishing: Hershey PA. p.20.
[84] H. Dragomirescu and R. S. Sharma, "Operationalising the Sustainable Knowledge Society Concept through a Multi-dimensional Scorecard", in (eds.), M. D. Lytras et al., *Best Practices for the Knowledge Society: Knowledge, Learning, Development and Technology for All* , Springer, Berlin, 2009 p. 335.
[85] ITU, *Measuring the Information Society Report 2017*, Volume 1, Geneva: Switzerland, pp. 95. 106.
[86] M. Waters, Daniel Bell, Routledge: London, p. 116.
[87] P. Blasi, "The European University – Towards a Wisdom-Based Society", *Higher Education in Europe*, 31(4), p. 403.
[88] J. Servaes & N. Carpentier, "Introduction: Steps to Achieve a Sustainable Information Society", in (eds.), by J. Servaes and Nico Carpentier, *Towards a Sustainable Information Society*, Intellect Books: Bristol, 2006, pp. 5-6.
[89] M. Castells, "The Network Society: from Knowledge to Policy", in (eds.) M. Castells and G. Cardoso (eds.), *The Network Society: From Knowledge to Policy*.Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005, pp. 7-16.
[90] J. A.G.M. van Dijk, *The Network Society: Social Aspects of New Media*, Sage Publications: London, 2006, p. 20.
[91] AIMS, "Information and Communication Technologies (ICT)", http://aims.fao.org/information-and-communication-technologies-ict,
[92] D. Lupton, "Introducing digital sociology", https://www.researchgate.net/publication/248381396, p. 2.
[93] D. Lupton, *Digital Sociology*, Routledge: London, 2015.
[94] E. Brynjolfsson and B. Kahin (eds.), *Understanding the Digital Economy*, The MIT Press, Cambridge, Massachusetts, 2000, p. 2.
[95] J. Suh and D. H. C. Chen (eds.), *Korea as a knowledge economy: evolutionary process and lessons learned*, The World Bank: Washington, 2007, pp. 3-4.
[96] C. Dahlman and A. Utz, *India and the Knowledge Economy Leveraging Strengths and Opportunities*, The World Bank: Washington, p. 9.
[97] B. Johansson et al. (eds.), *The Emerging Digital Economy: Entrepreneurship, Clusters, and Policy*, Springer Berlin, 2006, p.3.
[98] ODI (Overseas Development Institute), "Knowledge Economy", Retrieved fromhttps://www.odi.org/publications/5693-knowledge-economy-framework Framework, January 2009.
[99] R. D. Atkinson & Andrew S. Mckay**,** *Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution*, ITIF (The Information Technology and Innovation Foundation): Washington, 2007, p. 7.
[100] E. G. Carayannis and C. M. Sipp, *e-Development toward the Knowledge Economy*. Palgrave Macmillan: Hampshire, 2006, p. 12.
[101] ITU, *Measuring Information Society Report 2015*, Geneva: Switzerland, 2015, pp.3-4.
[102] UNCTAD (United Nations Conference on Trade and Development), *Digital Economy Report 2019*, United Nations Publications, New York, 2019,pp, 4,8,36.
[103] OECD (Organization for Economic Co-operation and Development), *Measuring the Digital Economy: A New Perspective*, OECD Publishing: Paris, 2014, p. 26.
[104] M. Castells, *The Internet Galaxy*: *Reflections on the Internet, Business, and Society*:, Oxford University Press: Oxford, p. 1.
[105] E. Isin and E. Ruppert, Being *digital citizens*, Rowman & Littlefield International: London, 2015, p. 7, 9.
[106] S. Hinduja, "Theory and Policy in Online Privacy", *Knowledge, Technology, & Policy*, Spring 2004, Vol. 17, No. 1, p. 38.
[107] Tes Teach, *Copy Of History Of The Internet - Lessons - Tes Teach*, https://www.google.com/search?q=History+of+the+Internet&sa=X&stick=H4sIAAAAAAAAAOOQUeLWz9U3MDS0zDLNTjESycwrS80ryczPU8hPU8hLLSnPL8qOEsovykzPBAtl5pWkFgHFTzEi6zvFyAnm5WSbVZ1i5ACxLYwsyqBM84yqbCjTuCin5BejiCcWWxaxintkFpfkF1WCBEsyUhU8oXYBAHMOb-KlAAAA&biw=1366&bih=604&tbm=isch&source=iu&ictx=1&fir=6DEk65o-vHHrlM%253A%252CMHDuCo42VmcHKM%252C_&vet=1&usg=AI4_-kS284FuGyso5lo9bdMndMVKDZLsnQ&ved=2ahUKEwi7_M2f7P7oAhUyxjgGHYDBDIQQ_h0wIHoECAUQBw#imgrc=_d1GeFLzARnpTM
[108] Ventcube, https://ventcube.com/history-of-the-internet-timeline/
[109] Simon Kemp,*Digital trends 2019: Every single stat you need to know about the internet*, https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet/
[110] ITU, Measuring *Digital Development Facts and Figures 2019*, Geneva: Switzerland, 2019, p. 1.
[111] J. Ryan, *A History of The Internet and the Digital Future*, Reaktion books, London, 2010, p.7.
[112] Internet Society, *2019 Internet society Global Internet Report*, https://future.internetsociety.org/2019/, pp. 18-29.
[113] Christian Fuchs, *Internet and Society Social Theory in theInformation Age*,Routledge New York, 2008, p. 1
[114] Internet Society, 2017 *Global Internet Report*, internetsociety.org, p. 20.
[115] Deloitte Touche Tohmatsu India LLP (DTTILLP), Decoding *National Digital Communications Policy (NDCP)*, 2018, p. 1.
[116] S. Rogerson. "Information Integrity in the Information Age", in (eds.), D. M. Haftor and A. Mirijamdotter, *Information and Communication Technologies, Society and Human Beings: Theory and Framework*, InformatIon Science Reference: Hershey, 2011, p. 339.
[117] R. Pintér, "Conceptualizing information society as risk society", *PeriodicaPolytechnica Ser. Soc. Man. Sci*, 11(1),2003, pp. 35-44.
[118] D. Gritzalis et al, "Roles of ICT in the InformationSociety", in (eds.) W.Shrum et al., *Past, Present and Future of Research in the InformationSociety*, 2007 Springer Science+Business Media, LLC, 2007, pp.75-95.
[119] S. K. Sharma "Socio-Economic Impacts and Influences of E-Commerce in a Digital Economy", in (eds.) H.S. Kehal and V.P. Singh, *Digital Economy: Impacts, Influences, and Challenge*, Idea Group Publishing: Hershey, 2005, p. 2.
[120] James Curran, "Reinterpreting the internet" , in (eds.) J. Curran et al.,, *Misunderstanding the Internet*, Routledge, New York, 2012, pp. 3-33.

©IJRASET: All Rights are Reserved

[121] R.J. Deibert, "Risking Security: Policies and Paradoxes of Cyberspace Security", International Political Sociology, 2010, 4, pp. 15–32.
[122] R. M. Unger, *The Knowledge Economy*, Verso: London, 2019, p.6.
[123] W. J. Schünemann and Max-Otto Baumann, *Privacy, Data Protection and Cybersecurity in Europe*, Springer: Switzerland, 2017, p. 1
[124] A. Ptak, "Cloud computing systems in information society - The European Enterprises towards Technological Advancement. Comparative rough set analysis", *Applied Mechanics and Materials*, 795, 2015, p.171.
[125] A. Alaqra et al., "Signatures for Privacy, Trust and Accountability in the Cloud: Applications and Requirements", in (eds.), D. Aspinall et al. (eds.), Privacy and Identity Management Time for a Revolution?, Springer: Switzerland, 2016, pp-79.80.
[126] A. Liew, "DIKIW: Data, Information, Knowledge, Intelligence, Wisdom and their Interrelationships", Business Management Dynamics, 2(10), 2013, 49-62.
[127] S. Baskarada and A. Koronios, "Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension", *Australasian Journal of Information Systems*, 18(1), pp. 5-24.
[128] G. Jifa, "Data, Information, Knowledge, wisdom and meta-synthesis of wisdom-comment on wisdom global and wisdom cities", *Procedia Computer Science* , 2013, 17, pp. 713 – 19.
[129] G. Bellinger et al., "Data, Information, Knowledge, and Wisdom", https://www.google.com/search?ei=lLT0Xs8M84zj4Q_3mbPoBA&q=bellinger-data+information+knowledge+and+wisdom&oq=bellinger-data+information+knowledge+and+wisdom&gs_lcp=CgZwc3ktYWIQDDIGCAAQCBAeOgQIABANOgYIABANEB46CAgAEAgQBxAeUKJVWOGMAWCTpgFoAHAAeACAAZMBiAHxCZIBBDAuMTCYAQCgAQGqAQdnd3Mtd2l6&sclient=psy-ab&ved=0ahUKEwjPpp3Dlp3qAhVzxjgGHffMDE0Q4dUDCAs, Retrieved on June 12, 2020, pp. 1-3.
[130] Jonathan Hey, "The Data, Information, Knowledge, Wisdom Chain: The Metaphorical link", https://www.google.com/search?source=hp&ei=gLb0XvmnMqqb4-EPnfGVoA4&q=The+Data%2C+Information%2C+Knowledge%2C+Wisdom+Chain%3A+The+Metaphorical+link&oq=The+Data%2C+Information%2C+Knowledge%2C+Wisdom+Chain%3A+The+Metaphorical+link&gs_lcp=CgZwc3ktYWIQDDICCABQtxZYtxZgnh9oAHAAeACAAWmIAWmSAQMwLjGYAQCgAQKgAQGqAQdnd3Mtd2l6&sclient=psy-ab&ved=0ahUKEwj555yumJ3qAhWqzTgGHZ14BeQQ4dUDCAY 2003.
[131] T. Lindsay and J. Ferris, "Characteristics of Data, Information, Knowledge, and Wisdom", (eds.), P.H. Sydenham and R. Thorn, *Handbook of System Design*, Vol. 3, Wiley: New York, 2005, p. 234.
[132] D. E. Holmes, Big Data: A very Short Introduction, Oxford University Press: Oxford, 2017.
[133] R. Behera et al., "Linkage-based Social Network Analysis in Distributed Platform", in (eds.), M. Panda et al., Big *data analytics: A social network approach*, CRC Press: Florida, 2019, pp. 10-2.
[134] C. Fuchs and D. Chandler, 'Introduction: Big Data Capitalism – Politics, Activism, and Theory', in (eds.), D. Chandler and C. Fuchs,*Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*, University of Westminster Press: London, 2019, p. 2.
[135] B. George and J. Paul (eds.), *Digital Transformation in Business and Society: Theory and Cases*, Springer: Switzerland, 2020, ppp. 1,.3.
[136] T.M. Payton and T. Claypoole, *Privacy in the Age of Big Data*, Rowman & Littlefield: Lanham, 2014.
[137] N. Patrignani et al., "Forget About Privacy … or Not?", in (eds.), M. Hansen et al., *Privacy and Identity Management: The Smart Revolution*, Springer: Switzerland, 2018, p. 77.
[138] D. Rodriguez-Lonebear, 'Building a data revolution in Indian country', in (eds.), T. Kukutai and J.Taylor, *Indigenous Data Sovereignty: Toward an Agenda*, ANU Press: Australia, 2016, pp. xxii, 253.
[139] R. Kitchin, *The Data Revolution: Bid Data, Open Data, Data Infrastructures and Their Consequences*, Sage: London, 2014.
[140] R. Simanowski, *Data Love : the seduction and betrayal of digital technologies*, Columbia University Press: New York, 2016.p. xii.
[141] W.H. Dutton (ed.), *Society on the Line: Information Politics in the Digital Age*, Oxford University Press: Oxford, 1999, p. 347.
[142] E. M. Newton and S. L. Pfleeger, "Information Technology Trends To 2020", in (eds.), R. Silberglitt et al., *The Global Technology Revolution 2020, In-Depth Analyses*, Rand: RAND Corporation, 2006, p.180.
[143] Bruce Schneier, *Data and Goliath The Hidden Battles to Collect Your Data and Control Your World*, W.W.Norton & Company: New York, 2015.
[144] J. van Dijck, "Foreward", in (eds.),M. Tobias Schafer & Karin van Es, *The Datafied Society: Studying Culture through Data*, Amsterdam University Press: Amsterdam 2017, p.11.
[145] M. Tobias Schafer & Karin van Es, *The Datafied Society: Studying Culture through Data*, Amsterdam University Press: Amsterdam 2017, p.13.
[146] European Commission, "Towards a common European data space", Brussels COM(2018) 232 final, 2018, pp. 2-3.
[147] A. Najmaei, **"**Understanding Business Models on the Cloud", in (ed.), M. Khosrow-Pour, *Encyclopedia of Information Science and Technology*, IGI Global: Hershey PA, USA, 2018, p. 1145.
[148] Dan Ciuriak and Maria Ptashkina, "Leveraging the Digital Transformation for Development: A Global South Strategy for the Data-driven Economy", *Centre for International Governance Innovation (2019)*, https://www.jstor.org/stable/resrep21057, Accessed on 13-04-2020.
[149] NIST, Nist Cloud Computing Standars Roadmap, Special Publication 500-291, Version 2, http://dx.doi.org/10.6028/NIST.SP.500-291r2, p. 21.
[150] N. Venkataramanan and A. Shriram, Data privacy: principles and practice, Data privacy : principles and practice,CRC Press: Boca Raton, FL, p. 1.
[151] N. Raza et al., "Security and management framework for an organization operating in cloud environment", Annals of Telecommunication. 72, 2017, pp. 325-328.
[152] P. C. K. Hung et al., "Privacy: Definition", in (eds.), L. Liu •and M. Tamer Özsu, *Encyclopedia of Database Systems*, Springer Science+Business Media, LLC: New York, 2018, p. 2801.
[153] P. Jain et al., "Big data privacy: a technological perspective and review" *Journal of Big Data*, 3(25), 2016, pp. 3-4.
[154] A. Kumar and R, Kumar, "Privacy Preservation of Electronic Health Record: Current Status and Future Direction", in (eds.), B. Gupta et al., *Handbook of Computer Networks and Cyber Security Principles and Paradigms*, Springer: Switzerland, 2020, p. 721
[155] L.D.Koontz (ed.), *Information Privacy in The Evolving Healthcare Environment*, CRC Press: Boca Raton, 2017, p.70.
[156] D. Gonzalez, *Managing Online Risk : Apps, Mobile, and Social Media Security*, Elsevier: Amsterdam, 2015, p. 109.
[157] L. Kacha and A. Zitouni, "An Overview on Data Security in Cloud Computing", in (eds.)R, Silhavy et al., *Cybernetics Approaches in Intelligent systems*, Springer: Switzerland, 2018, pp. 254-8.

©IJRASET: All Rights are Reserved

[158] V.Kumar et al, "A Data-Centric View of Cloud Security", in (eds.) V. Kumar et al., *Data Security in Cloud Computing*, IET: London, 2017,pp. 9-13.
[159] N. Subramaniam and A. Jeyaraj, "Recent Security Challenges in Cloud Computing", *Computers and Electrical Engineering*, 71, 2018, pp. 37-40.
[160] Y. Sun et al, "Data Security and Privacy in Cloud Computing", *International Journal of Distributed Sensor Networks*", 10 (2014), pp. 1-9.
[161] Alrabaee et al.(eds.), " Preserving Database Privacy in Cloud Compting", in(eds.), *Recent Trends in Computer Networks and Distributed Systems Security*, Springer: Berlin, 2014, 485.
[162] M.V. Shabalala et al. (eds.), "Addressing Privacy in Cloud Computing Environment", in (eds.), A. Nungu et al., *e-Infrastructure and e-Services for Developing Countries*, Springer: Heidelberg, 144.
[163] A. Ghorbel et al., "Privacy in Cloud Computing Environments: A Survey and Research Challenges", *Journal of Supercomputer*, 73, 2017, pp. 2768-9, 2771.
[164] J. J. Trinckes, Jr., *How healthcare data privacy is almost dead ... and what can be done to revive it!!*, CRC Press: Boca Raton, FL ,2017, p. 263.
[165] D.S. Allison and M.A.M. Capretz, "Furthering the Growth of Cloud Computing by Providing Privacy as A Service", in (eds.), D.Kranzlmuller and A.M. Toja, *Information and Communication Technology for the Fight against Global Warming*, Springer: Verlag Berlin,2011, p. 68.
[166] Daniel J. Solove, *Understanding privacy*, Harvard University Press: Cambridge, 2008, p. 1.
[167] L. Koontz (ed.), *Information Privacy in the Evolving Healthcare Environment*, CRC Press: Boca Raton, FL, 2017.
[168] D. K. Mulligan et al., "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy", *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, 374(2083), 2016, pp. 10-11.
[169] R. Chandra, *The Right to Privacy with Special Reference to Information Technology Era*, YS Books International: New Delhi, 2017, p. 18.
[170] A. F. Westin, *Information Technology in a Democracy*, Harvard University Press: Cambridge, 1971, p. 2
[171] A. F. Weston, *Privacy and Freedom*, Atheneum: New York, 1968, p. 7.
[172] Irwin R. Kramer, "The Birth of Privacy Law: A Century SinceWarren And Brandeis", *Catholic University Law Review*, 39, 1990, p. 703.
[173] S. D. Warren and L. D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4(5), 1890, p. 195.
[174] H. Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy* 17, 1998, p.559.
[175] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books: Stanford, California, 2010, p. 127.
[176] Frances Grodzinsky and Herman T. Tavani, "Privacy in "The Cloud": Applying Nissenbaum's Theory of Contextual Integrity", *SIGCAS Computers and Society*, 31(1), 2011, pp. 45-6.
[177] ITU, *Privacy in Cloud Computing*, Geneva: Switzerland, 2012, p. 1.
[178] R. Hassan and S. Zawoad, "Privacy in the Cloud", in (eds.), S. Zeadally and M. Badra, *Privacy in a Digital, Networked World: Technologies, Implications and Solutions*, Springer: Heidelberg, 2015, p.142, 148,155-60.
[179] A.Cavoukian, "Privacy in the clouds", Identity in the Information Society, 1(1), p. 90.
[180] G. Danezis and S. Gurses, "A critical review of 10 years of Privacy Technology", Proceedings of Surveillance Cultures: A GlobalSurveillance Society?, 2010, p. 4.
[181] L. Arockiam et al., "Privacy in Cloud Computing: A Survey",in (eds.) N. Meghanathan, et al., *SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 321–330, 2012. © CS & IT-CSCP 2012*, DOI: 10.5121/csit.2012.2331, pp. 324-5.
[182] M.U. Shankar and A.V. Pawar, "Security and Privacy in Cloud Computing: A Survey", in (eds,), S.C. Satapathy et al. (eds.), *Proceedings of the 3rdInternational Conference onFrontiers of IntelligentComputing: Theory and Applications. (FICTA) 2014*, Vol. 2, Springer: Cham Heidelberg, 2015, pp. 3-4.
[183] B. Joshi et al., "Mitigating Data Segregation and Privacy in Cloud Computing", in (eds.), N. Modi et al., *Proceeding of International Conference on Communication and Network*s, Springer: Singapore, 2017, pp. 177-8, 181.
[184] Y. Sun et al., "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks, 6, 2014, pp. 3-4.
[185] T. Mather et al., *Cloud Security and Privacy*, O'Reilly: Cambridge, 2009, p.149-50.
[186] C. Kalloiatis, "Designing Privacy-Aware Systems in the Cloud", in S. Fischer-Hubner, *Trust, Privacy and Security in Digital Business*, Springer: Heidelberg, pp.115-7.
[187] A. Kitkowska et al., "Is It Harmful? Re-examining Privacy Concerns", in (eds.), M. Hansen et al., *Privacy and Identity Management*: *The Smart Revolution*, Springer: Switzerland, pp. 69-71.
[188] S. Pearson, "On the Relationship between the Different Methods to Address Privacy Issues in the Cloud", in (eds.), R. Meersman et al., On *the Move to Meaningful Internet Systems: OTM 2013 Conferences*, Springer: Verlag Berlin Heidelberg, 2013, p. 414.
[189] R. Kumar and R. Goyal, "On Cloud Security Requirements, Threats, Vulnerabilities and Countermeasures: A Survey", *Computer Science Review*, 33(2019), p. 11.
[190] P. Kalia, et al., "Analyzing Privacy Issues in Cloud Computing Using Trust Model', in (eds.), Krishna et al., *Proceedings of 2nd International Conference on Communication, Computing and Networking*, Springer: Singapore, 2019, p. 1043.
[191] OECD, "Guidelines governing the protection of privacy and transborder flows of personal data" , in OECD Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data, The OECD Privacy Framework, Pais: OECD, 2013, P. 14-5.
[192] Madrid Resolution , 'Data protection authorities from over 50 countries approve the "Madrid Resolution" on international privacy standards, Retrieve from https://www.google.com/search?source=hp&ei=IsHdXoX7K737z7sPwdqHuAY&q=madrid+resolution+data+protection&oq=mADRID+rEOLUTION+&gs_lcp=CgZwc3ktYWIQARgCMgQIABANMgYIABAWEB4yBggAEBYQHjIGCAAQFhAeMgYIABAWEB4yBggAEBYQHjoOCAAQ6gIQtAIQmgEQ5QI6BQgAEIMBOgUIABCxAzoCCAA6CAgAEBYQChAeOgYIABANEB46BQghEKABOggIABAIEA0QHlCyEVjuY2DlkwFoAXAAeACAAZgBiAHeD5IBBDAuMTeYAQCgAQGqAQdnd3Mtd2l6sAEG&sclient=psy-ab,
[193] B. Dzziminski and N.C. Gleeson, "Legal Aspects of Cloud Accountability'. in (eds.) M. Felici and C. Fernandez-Gago, *Accountability and Security in the Cloud*, Springer: Switzerland, 2015, pp.227, 240.
[194] S. Pearson, "Privacy, Security and Trust in Cloud Computing', in (eds.), S. Pearson and G. Yee, *Privacy and Security in Cloud Computing*, Springer-Verlag: London, 2013.
[195] M. D. M. L. Ruiz and Pedraza, "Privacy Risks in Cloud Computing", in(eds.), J. Kołodziej et al., *Intelligent Agents in Data Intensive Computing*, Springer: Switzerland, 2016, p. 178.

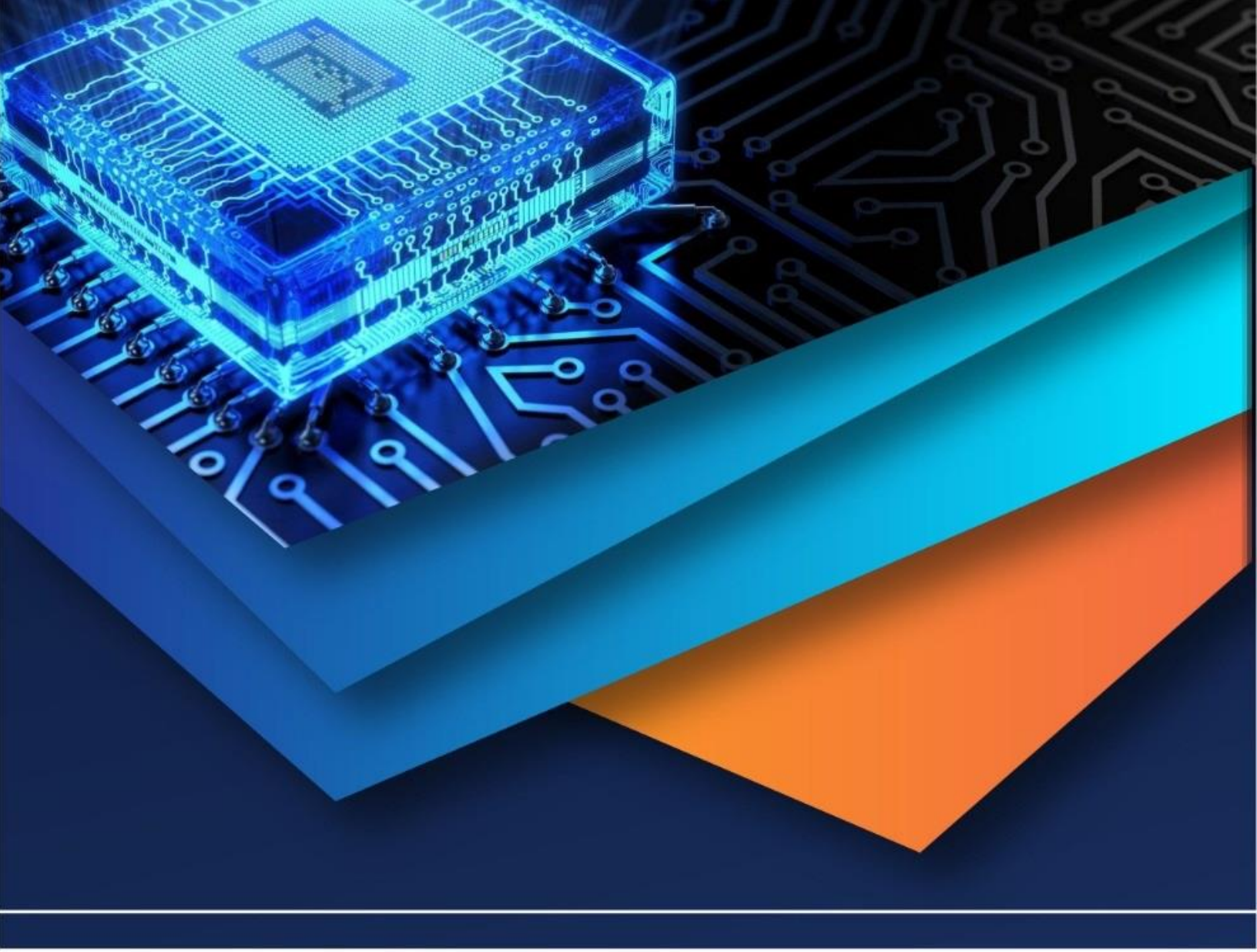
©IJRASET: All Rights are Reserved

[196] D.S. Allison and M. A.M. Capretz, "Furthering the Growth of Cloud Computing by Providing Privacy as a Service". in (eds.), D. Kranzlmller and A.M. Toja, *Information and Communication on Technology for the Fight against Global Warming*, Springer-Verlag:Berlin, 2011, pp. 75-6.
[197] M.V. Shabalala et al., "Addressing Privacy in Cloud Computing Environment", in (eds.), A. Nungu et al., *e-Infrastructure and e-Services for Developing Countries*, Springer Cham:Heidelberg, 2015, p. 152.
[198] ENISA (European Union Agency for Network and Information Security*), Privacy by design in big data An overview of privacy enhancing technologies in the era of big data analytics*: *Final*, VassilikaVouton: Greece, pp. 21-2.
[199] P.R. Kumar et al., "Privacy preserving security using biometrics in cloud Computing", *Multimedia Tools and Applications*volume 77, 2018,pp. 11017–39.
[200] Lijo V.P and S. Kalady, "Cloud Computing Privacy Issues and User-Centric Solution", (eds.) K.R. Venugopal and L.M. Patnaik,. *Computer Networks and Intelligent Computing*, Springer: Heidelberg, 2011, pp. 448-56.
[201] L.A. Cutillo and A. Lioy, "Towards Privacy-by-Design Peer-to-Peer Cloud Computing", in (eds.), S. Furnell et al., *Trust, Privacy, and Security in Digital Business*, Springer-Verlag: Berlin, 2013, pp. 85-96.
[202] V. Kavya et al., "A Survey on Data Auditing Approaches to Preserve Privacy and Data Integrity in Cloud Computing", in (eds.), P. Karrupusamy et al., *Sustainable Communication Networks and Application ICSCN 2019*, Springer Nature:Switzerland, pp. 108-18.
[203] V. Torraand G. Navarro-Arribas, "Data Privacy: A Survey of Results", in (eds.), G. Navarro-Arribas and V. Torra, Advanced Research in Data Privacy, Springer Cham: Heidelberg, 2015, pp. 27-37.
[204] V. Tchifilionova, "Security and Privacy Implications of Cloud Computing – Lost in the Cloud", in (eds.), Jan Camenisch et al., *Open Research Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2010*, Springer: Heidelberg, 2011, p. 157.
[205] J. Camenisch et al., "Preface", in (eds.), Jan Camenisch et al., *Digital Privacy, PRIME – Privacy and Identity Management for Europe*, Springer-Verlag: Berlin, 2011, pp. vii-viii.
[206] R. G. Taylor, "The Social Side of Security", in T. Kidd and I. L. Chen, *Social Information Technology: Connecting Society and Cultural Issues*, Information Science Reference: Hershey • New York, 2008, p. 143.
[207] J. Graham et al., *Cyber Security Essentials*, CRC Press: Boca Raton, 2011, pp. 1-6.
[208] M. D. M. L. Ruiz and J. Pedraza, "Privacy Risks in Cloud Computing", in (eds.), Joanna Kołodziej et al., *Intelligent Agents in Data-intensive Computing*, Springer Cham: Heidelberg, 2016, pp. 170-71.
[209] A. Azmoodeh and A. Dehghantanha, **"**Big Data and Privacy: Challenges and Opportunities", in (eds.), K-K. R. Choo and A. Dehghantanha, *Handbook of Big Data Privacy*, Springer: Switzerland, 2020, p. 1.
[210] L. Taylor et al., "Introduction: A New Perspective on Privacy", in (eds.), L Taylor et al., *Group Privacy New Challenges of Data Technologies*, Springer: Switzerland, 2017, pp. 3-4.
[211] J. Rauhofer, "Privacy is dead, get over it.Information privacy and the dream of a risk-free society", *Information& Communications Technology Law*, 17(3), p. 188.
[212] V. Packard, *The Naked Society*, David McKay: New York, 1964, p.29.
[213] J. Domingo-Ferrer et al., "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges", *Computer Communications* 140–141, 2019, pp. 38–60.
[214] C. Dhasarathan et al., "A secure data privacy preservation for on-demand cloud service",*Journal of King Saud University – Engineering Sciences*, 29, 2017, pp. 144–50.
[215] D. Dempsey and F. Kelliher, *Industry Trends in Cloud Computing: Alternative Business-to-Business Revenue Models*, Palgrave Macmillan: Springer Nature: Switzerland, 2018.
[216] J. Halton, "The Anatomy of Computing", in (ed,), T. Forester, *The Information Technology Revolution*, The MIT Press: Cambridge, Massachusetts, p. 4.
[217] David M. Berry, The Philosophy of Software: Code and Mediation in the Digital Age, Palgrave Macmillan: New York, 2011, p. 3.
[218] L. D. Ball, 'Computer Crime', in (ed,), T. Forester, The Information Technology Revolution, The MIT Press: Cambridge, Massachusetts, p. 533.
[219] P. C. van Oorschot, *Computer Security and the Internet: Tools and Jewels*, Springer: Switzerland, 2020, p. 25.
[220] Stephen D. Tansey, Business, Information Technology and Society, Routledge: London, 2003, p. 106.
[221] Rob Sobers,110 Must-Know Cybersecurity Statistics for 2020, Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/020 **,** Varonis.
[222] CA with E. Geier and J. Geier, Simple Computer Security Disinfect Your PC, **Wiley:** Indianapolis, IN, 2007.
[223] C. Easttom and D. J. Taylor (2011), *Computer Crime, Investigation and the Law*, Course Technology: Boston, 2011, pp.38, 43, 50.
[224] Paul DiMaggio et al, "Social Implications of the Internet", *Annual Review of Sociology* 27, 2001, pp. 307-24..
[225] M.H. Zaharia, "A Paradigm Shift in Cyberspace Security", in (eds.) B. Akhgar and H.R. Arabnia, *Emerging Trends in ICT Security*, Amsterdam: Elsevier 2014, p. 443.
[226] C.S.R. Prabhu, "Big Data Analytics" in (eds.) C.S.R. Prabhu et al., *Big Data Analytics: Systems, Algorithms, Applications*, Springer Nature: Singapore, 2019, pp. 2-3.
[227] P.W. Singer and A. Friedman, *Cybersecurity and Cyber War*, Oxford:Oxford University Press, 2014, pp. 250-51.
[228] R. Shah, "Law Enforcement and Data Privacy: A Forward-Looking Approach" *The Yale Law Journal*, 125 (2), 2015, p.. 543.
[229] Christian Fuchs, *Internet and Society Social Theory in the Information Age*, Routledge: New York, 2008, p. 1.
[230] J. A. Bargh and K. Y. A. McKenna, "The Internet and Social Life"*Annual Review of Psychology*, 55, 2004, pp. 573–90.
[231] B. Wellman and C. Haythornthwaite, *The Internet in Everyday Life*, Blackwell: Oxford, 2002.
[232] S.Ghernaouti, "The role of CBMs in a renewed vision of international cybersecurity: prospects for a global response and an international treaty", in H. I. Touré, *The Quest for Cyber Confidence*, ITU: Geneva, Switzerland, 2014, pp.. 13, 89.
[233] S. K. Sharma "Socio-Economic Impacts and Influences of E-Commerce in a Digital Economy", in (eds.), H. S. Kehal and V. P. Singh, *Digital Economy: Impacts, Influences, and Challenges*, Hershey PA. Idea Group Publishing: Hershey PA, 2005, p. 2.
[234] S. Chapman and G. S. Dhillon, "Privacy and the Internet: The Case of DoubleClick, Inc.", in (ed.), G. S. Dhillon, *Social Responsibility in the Information Age: Issues and Controversies*, Idea Group Publishing: Hershey PA, 2002, p. 86.
[235] D. Lyon, *The Electronic Eye: The Rise of Surveillance Society*, University of Minnesota Press: Minneapolis, MN, 1994.

©IJRASET: All Rights are Reserved

[236] D. Lyon, *Surveillance Society: Monitoring Everyday Life*, Open University Press, 2001.
[237] D. Lyon, *Surveillance, Privacy and the Globalization of Personal Information*, McGill-Qeen's University Press 2010.
[238] D. Lyon (ed.), *Theorizing Surveillance*, Willan Publishing: Portland, Oregon, 2006.
[239] D. Lyon, "Surveillance Society", Talk for Festival delDiritto, Piacenza, Italia: September 28 2008, https://www.google.com/search?biw=1366&bih=598&ei=LOPoXtG5PNOK4-EPw-yq0A0&q=D.+Lyon-surveillance+society+--Talk+for+Festival+del+Diritto&oq=D.+Lyon-surveillance+society+--Talk+for+Festival+del+Diritto&gs_lcp=CgZwc3ktYWIQDDoFCCEQoAE6BggAEBYQHlCQ4gJYnpMDYIqgA2gBcAB4AIABlAGIAasFkgEDMS41mAEAoAEBoAECqgEHZ3dzLXdpeg&sclient=psy-ab&ved=0ahUKEwjR_7Sj0YbqAhVTxTgGHUO2CtoQ4dUDCAs.
[240] J.K. Petersen, *Handbook of Surveillance Technologies*, C.R. Press: Boca Raton, 2012.
[241] G. T. Marx, "What's new about the "new surveillance"? Classifying for Change and Continuity", *Surveillance & Society*, 1 (1), 2002, p. 12.
[242] C. Fuchs et al., "Introduction:Internet and Surveillance", in (eds.), C. Fuchs et al., *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, Routledge: New York, 2012, p. 1.
[243] L. Kacha(&) and A. Zitouni, "An Overview on Data Security in Cloud Computing", in (eds.), R. Silhavy et al., *Cybernetics Approaches in Intelligent Systems*, Springer: Switzerland, 2018, p. 253.
[244] R. Pinter, "Conceptualizing information society as risk society", *PERIODICA Polytechnica Ser. Soc. Man*. SCI., 11(1), 2003, pp. 40, 43.
[245] Klaus Brunnstein, "The Information/Knowledge society as Risk Society: Assessing and Enforcing IT safety and security standards for IT systems: about responsibility of experts and governments", in (eds.), P. Gujon et al., The *Information Society: Innovations, Legitimacy, Ethics and Democracy*, Springer: Boston, 2007, pp. 30-31.
[246] Beck, U., *Risk Society: Towards a New Modernity*, Sage: London, 1996, pp. 19, 78-9.
[247] Beck, U., "Risk Society and the Provident State", in (eds.) S. Lash et al., *Risk Environment and Modernity*, Sage: London. 1996, p. 28.
[248] J. Urry, 'Preface' in U. Beck, Ulrich Beck: Pioneer in Cosmopolitan Sociology and Risk Society, Springer: Heidelberg, 2014, p. vi.
[249] U. Beck, *World Risk Society*, Polity Press: Cambridge, 1999, pp. 76-7.
[250] ITU,Privacy in Cloud Computing: ITU-T Technology Watch Report, https://www.itu.int/oth/T2301000016/en, Retrieved on 18 June 2020, pp. 1, 17.
[251] D. Aspinall et al., *Privacy and Identity Management: Time for a Revolution?*, Springer: Switzerland, 2016, p. v.
[252] B. Schneier, *Schneier on Security*,Wiley: Indianapolis, IN, 2008, pp. 64-5.
[253] T. W. Edgar, and D.O. Manz, *Research Methods for Cyber Security*, Syngress: Cambridge, MA, 2017, p. 71.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)