CLOUD COMPUTING THREATS AND RISKS: UNCERTAINTY AND UNCONROLLABILITY IN THE RISK SOCETY

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

Abstract: As the Fourth Industrial Revolution era is now constantly progressing, the emergence of Cloud Computing, the Internet of Things, and Big Data is fast changing the computer domain. Accordingly, the computing tasks and processes are getting bigger and more complicated than ever before. In particular Cloud Computing (hereafter abbreviated as CC) is turning out to be a labyrinth in spite of its enormous advantages that it offers to its stake holders—both the individuals and organizations-- in today’s informational environment of the networked society. CC, as a popular and promising domain of technological paradigm, is now globally established following the availability of high capacity network system, less expensive computers and scalable storage tools, reliable hardware virtualization, and necessaryservice oriented architectural frameworks - all ready to instantly deliver various services on demand. Be that as it may, the character of CC is in a way dialectical and, accordingly, the main objective of the present paper is to undertake, from an interdisciplinary cyber-behavioural perspective, a modest attempt to frame a critical discourse mainly of its threats, vulnerabilities and risks that haunt CC services. These CC issues make it impossible to achieve end–to-end security, on the one hand, and, at one and the same time, further strengthen, on the other hand, the process of transforming late modern society into what is known as risk society.

Key words: **Cloud Computing, Threats and Risks, Challenges and Countermeasures, Human Factors, and Risk Society.**

I:INTRODUCTION

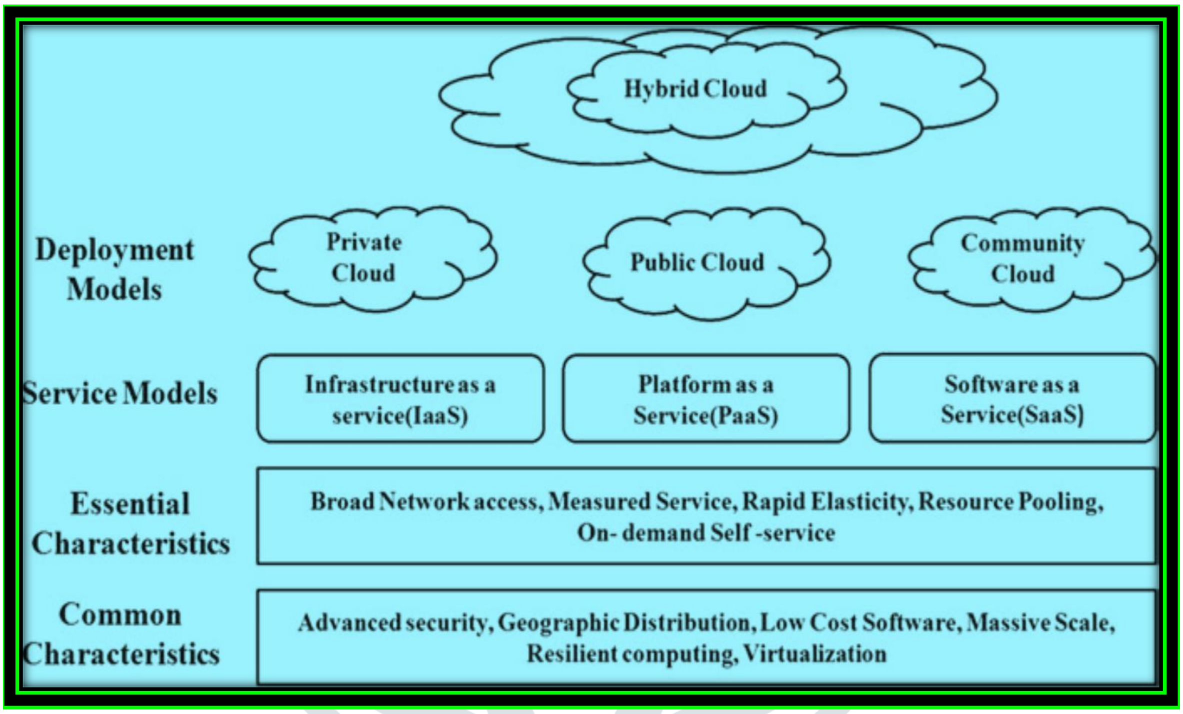
Renaissance was a historic transformation that took place in Europe between 14th and 17th centuries. But it was the First Industrial Revolution(I.1.0) in the 1760s, which witnessed the arrival of a series of innovations (viz. steam engine, machine tools etc.) gave rise to mechanized production and hence accelerated manufacturing productivity and development first in Europe and United States and later in other parts of the world. The Second Industrial Revolution (I.2.0) around 1870s transformed production with technological innovations like electricity, assembly line, conveyer belts etc., resulting in what is known as mass production. The Third Industrial Revolution (I.3.0), occurring in the 1960s, strengthened the industrial scenario with coming of communication technologies with energy regimes especially renewable electricity[2]. Schwab says that this Third Industrial Revolution is called ‘the computer or digital revolution because it was catalysed by the development of semiconductors, mainframe computing (1960s), personal computing (1970s and 80s) and the internet (1990s)’[3]. It saw the integration of manufacturing with electronics leading to the era of NC, CNC, DNC classes of automated production machinery. Driven by forces of globalization and market economy, but based on what was achieved earlier, came the Fourth Industrial Revolution (I. 4.0) sometimes called “cyber-physical systems”, a whole bunch ofenabling technologies (Internet, Information and Communication Technologies or ICTs and physical Machinery) and their fusion. The importance of this Revolution is epochal. As Schwab underlines: ‘Fourth Industrial Revolution technologies are truly disruptive—they upend existing ways of sensing, calculating, organizing, acting and delivering. They represent entirely new ways of creating value for organizations and citizens. They will, over time, transform all the systems we take for granted today—from the way we produce and transport goods and services, to the way wecommunicate, theway we collaborate, and the way we experience the world around us.’[4].

In any case, of the Fourth Industrial Revolution (I.4.0) technologies came the concepts suchas Internet of things (IoT), industrial Internet of things (IIoT), cobot (collaborative robot), big data, cloud computing, virtualmanufacturing,and 3D printing, artificial intelligence, biotechnology and others [3]. The Fourth Industrial Revolution is integrallyand specifically connected with such disciplinary areas, argue Kumar and others, ‘asintelligent 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’[5]. How the CC is connected to Robotics, which emerged during the Fourth Industrial Revolution, 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’ [6].Inbrief, ‘Cloud computing combines the best of the mainframe era with the best of the PC-enabled client-server era along with the Internet era’ [7].

The remainder of present paper is as follows. In section **II** an overview of CC is provided. In section **III** CC security is discussed with reference to (a) threats and their solution, and (b) risks and their countermeasures. In section **IV** increasing challenges or deficits in countermeasures are taken up emphasizing uncertainty in CC. In the final section **V** the relationship between CC and risk society is conceptualized to affirm the dialectical nature of both CC and risk society which has both assets and liabilities. The CC is analysed as a component of risk society in this modern historical period.

II: WHAT IS CLOUD COMPUTING?

CC did not emerge suddenly. It went through a process of evolution between the 1960s and 1990s, when the internet only started to offer significant bandwidth [8].It is very difficult to define what CC is because the there is no consensus among concerned experts on its definition. According to Sharma and others, 'Cloud Computing refers to both the application delivered as services over the internet, the hardware and systemssoftware in the data centers that provide those services'[9].The utility-oriented nature of cloud computing is defined by Buyya et al. 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'[10].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'**[**1]. NIST also enumerates five characteristics such as *On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, and Measured Service* [1]. CC has three service offerings and four development models, as shown in the next **Table 1** below [11].



	Hybrid Cloud		
Deployment Models	Private Cloud	Public Cloud	Community Cloud
Service Models	Infrastructure as a service(IaaS)	Platform as a Service(PaaS)	Software as a Service(SaaS)
Essential Characteristics	Broad Network access, Measured Service, Rapid Elasticity, Resource Pooling, On- demand Self -service		
Common Characteristics	Advanced security, Geographic Distribution, Low Cost Software, Massive Scale, Resilient computing, Virtualization		

Table 1 NIST Visual Model for Cloud Computing

Of the three service offering, the first is *Infrastructure as a Service* (IaaS) which provides resources like servers, virtual machines, data centre space and operating system. The resources can be rentedand arescalable on payment as per amount of usage. These are often managed by Application Programming Interface (API). Second, there is what is called *Platform as a Service* (PaaS)which enables the customer to execute the software such as operative system, database, server and programming language environment etc. It refers to 'the delivery of computing solution for software development including a running environment and lifecycle management software. This allows customers to develop new applications using APIs deployed and configurable remotely' [12]. Finally, the *Software as a Service* (SaaS),which is widely used, refers to the delivery of application as a service running on a cloud infrastructure. It is available on demand and paid for on usage basis to many clients 'through a thin client interface such as a web browser' [13]. The following **Figure 1**illustrates different aspects three CC service offerings provided in the DevTeam.Space Product Development Blog [14].

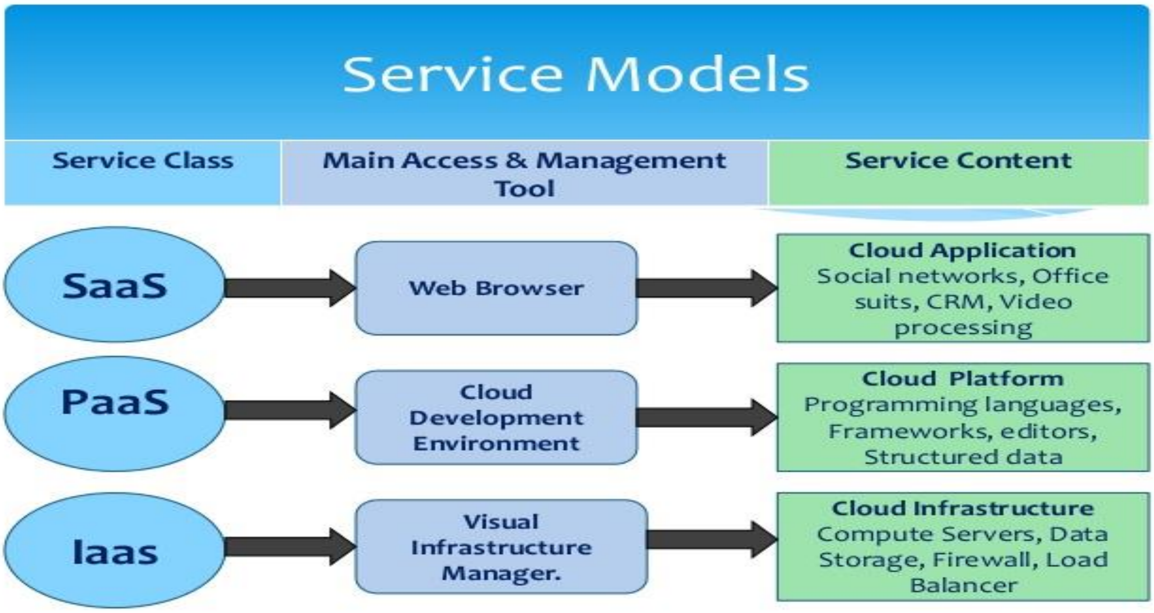

Service Models
Service Class
Main Access & Management Tool
Service Content
SaaS
Web Browser
Cloud Application
Social networks, Office suits, CRM, Video processing
PaaS
Cloud Development Environment
Cloud Platform
Programming languages, Frameworks, editors, Structured data
Iaas
Visual Infrastructure Manager.
Cloud Infrastructure
Compute Servers, Data Storage, Firewall, Load Balancer

Figure 1 Different Aspects of SaaS, PaaS, and Iaas

In **Figure2** Murugesan and Bojanova (2016) depict capability and controllability of the user in each of the three servicing models that the user has the capability and control over the CC services and infrastructure[15].

Service model	Capability offered to the user	Controllability by users
Software as aservice (SaaS	Use of applications that run on the loud.	Limited application configuration settings, but no control over underlying cloud infrastructure – network, servers, operating systems, storage, or individual application capabilities.
Platform as aservice (PaaS)	Deployment of applications onthe cloud infrastructure; may use supported programminglanguages, libraries, services, and tools.	The user has control of deployed applications and their environment settings, but no control of cloud infrastructure – network, servers, operating systems, or storage.
Infrastructure asa service (IaaS	Provisioning of processing, storage, networks, etc.; may deploy and run operating systems, applications, etc.	The user has control of operating systems, storage, and deployed applications running on virtualized resources assigned to the user, but no control over underlying cloud Infrastructure.

Figure 2 Cloud Computing Services Models in respect of user's capability and control

Of the three CC deployment models, one is *private cloud*, the cloud platform which is usually set up for exclusive of an organization which may have its own data center and thus can , manage, operate and control it.

In the *public cloud*, made available by any service provider, cloud services are made available to the desire entity of the public. It is less secure because the provider manages and controls it. In the *community cloud*, the infrastructure is shared by one or more communities having a shared purpose or mission. It can be owned and managed by one or more participants or by a third party. The hybrid cloud platform consists of at least two cloud infrastructures (private, public and community, or internal and external) whereby organizations can switch applications from one platform to another, such as from internal private cloud to a secure public cloud [16].The attributes of cloud models are shown below[17] in **Figure 3** by Amara (2017).

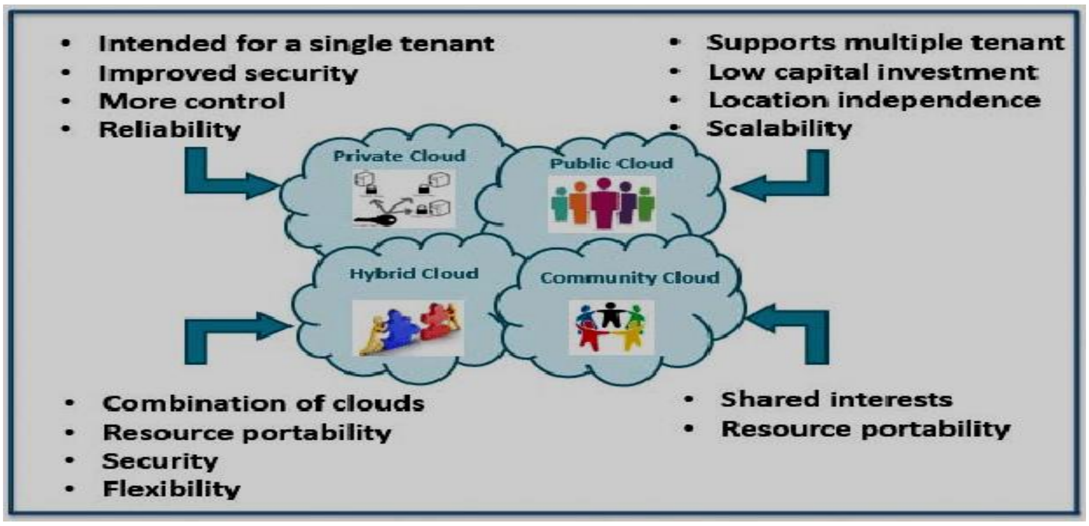


Figure 3attributes of cloud computing deployment models

II.CLOUD COMPUTING SECURITY

II. I. THREATS AND SOLUTIONS

Security challenges such as threats, vulnerabilities and risks, although at times confused, are almost a pervasive phenomenon in the CC services and computation processes. Necessarily, these terms need to be defined as precisely as possible keeping in view the fact that they are interrelated with each other.Bhowmik defines theconcepts as follows. Threat is ‘an event that can cause harm to a system. It can damage the system’s reliability and demote confidentiality, availability or integrity of information stored in the system. Threats can be malicious such as deliberate alteration of sensitive data or can be accidental such as unintentional deletion of a file or problem arisen from erroneous calculation’. Vulnerability refers to ‘some weaknesses or flaws in a system (hardware, software or process) that a threat may exploit to damage the system. It refers to security flaws that pose the threat to a system increasing the chance of an attack to be successful’. Finally, risk refers to ‘the ability of a threat to exploit vulnerabilities and thereby causing harm to the system. Risk occurs when threat and vulnerability overlap. It is the prospect of athreat to materialize’. Common threats to any computing system are eavesdropping (capturing data packets for sensitive information),fraud (altering data to make illegitimate gain), theft (stealing trade secret or data financial gain), sabotage (disrupting data integrity, DoS), and external attack (inserting a malicious code or virus) [18]. Dahbur provides an equation of the interrelation among them: Risk=Vulnerability x Threat x Impact x Likelihood, and also defines a countermeasure (e.g. strong authentication mechanism, computer antivirus software, or information security awareness). It isdesigned to mitigate the potential risk and can be ‘a policy, procedure, a software configuration, or hardware device that eliminates vulnerability or reduces the likelihood that a threat agent will be able to exploit vulnerability’ [19].

First of all, it is necessary to explain the fact that threats, vulnerabilities and risks rose in a historical context with the appearance of cyberspace--‘hallucinogenic parallel universe known as The Cybersphere’ [20] which, in turn, witnessed the arrival of cyber crimes of which cloud crime is a subset. As Brenner argues, cybercrime appeared with the coming of mainframe computers in the 1950s and 1960s, and rapidly changed since 1990 when internet and personal computers became widespread. Between 1990 and 2009 cybercrimes increased its incidence and complexity. It was followed‘professional, targeted attacks’ and replaced the malware ‘hobbyism’ of the 1990s. With the end of the first decade of the 21st century, cybercrime (Cyberspace+Crime=Cybercrime) became big business on a global scale. Very simply defined, cybercrime involves engagement with unlawful conduct that threatens order. It differs from crimes in terms of methods used. ‘Criminals use guns, whereas cybercriminals use computer technology. Most of the cybercrime we see today simply represents the migration of real-world crime into cyberspace. Cyberspace becomes the tool criminals use to commit old crimes in new ways’ [21]. Cybercrime generally refers, as Hill and Marion say, ‘to acts that involve criminal uses of the Internet or other networked systems to cause harm to others or some form of a disturbance. It can include any criminal activity—not only on computers, networks, or the Internet but also on mobile phones orother personal devices—that is intended to cause harm to others. These are illegal activities that are conducted through global electronic networks. In short, the term “cybercrime” refers to methods by which computers or other electronic devices are used to carry out criminal activity and cause harm to others’. They also cite examples of cybercrimes and their attacks which include unauthorized access to a computer system, illegal interception or alteration of data, or misuse of electronic devices the theft of intellectual property, trade secret, deliberately disrupt processing or acts of espionage to make unauthorized copies of classified data,, stealing money from bank accounts, creating viruses, postingconfidential business information on the Internet, committing identity theft or fraud, , money launderingand counterfeiting, and committing denial-of-service, malware; fake emails or websites; identity theft;cyberbullying, stalking, or harassment; hacking, credit card theft; or phishing etc.[22]. The challenges or features of digital technology which facilitate cybercrimes and hamper law enforcement are scale, accessibility, anonymity, portability and transferability, global reach, and absence of capable guardians [23] .It is predicted that the number of viruses and Trojans for mobile devices such as smartphones, tablets, iPads and iPods, and whatever else is available on mobile platforms will swell systematically in the near future [24].Before examining in general cloud computing threats and their solutions in particular it is necessary to spell out and distinguish between cybercrime and what constitutes a cloud crime that follows from cyber attacks on cloud computing. The following **Table 2** by Brar and Kumar [25] classifies cybercrimes.

Cyberviolence	Denial of Service/Distributed Denial of Service
Cyberpeddler	Keylogger and social engineering
Cybertrespass	Traffic Analysis, Eavesdropping, snooping, Password attacks, SQL Injection, Salami Attack, and Data Diddling
Cybersquatting	Session Hijacking

Table 2 Classification of cyber attackson the basis of cyber crimes

Technology by Modus operandi	Crimes against the machines	Crimes using the machines	Crimes in the machine
Cyber-assisted	Social engineering password theft	P2P fraud	Informational crime –terror handbook
Cyber -enabled		Mass Frauds	
Cyber-dependent	DDoSAttacks, Mass hacks	Phishing, Ransomware	SNM, Hate speech

Table 3 A Cybercrime Matrix(Mediation by technology v modus operandi)

Wall shows, in **Table 3**, a cybercrime matrix in which cloud crime is a subset of cybercrime [26]. Wall suggests that cybercrimes describe ‘a transformational process from one state (offline) to another (online) - a process that is continuing into the future with the development of cloud technologies and the internet of things’ and also those crimes are mediated by technologies generating new cybercrimes by ‘a number of different *modus operandi* (objectives and intents)’.Cyber assisted crimes, which use internet, will still occur if internet is removed (searching for how to kill and dispose of the body). Cyber-dependent crimes will disappear if the internet (networked technology) is taken away. In between there are range of hybrid cyber-enabled crimes which are given ‘a global reach by the internet, see for example the Ponzi frauds and pyramid selling scheme scams. Take away the internet, and these crimes still happen, but at a much more localized level, and they lose the global, informational and distributed lift that is characteristic of ‘cyber’’.Further, Wall states that ‘cloud technologies are impacting upon criminal behavior online in three transformational ways; by increasingcomputing power, they increase storage capacity and reducing the cost of computing power. This means that(cyber) criminals can commit a larger volume of more complex crimes at a reduced cost’. Visualizing a future scenario, Wall conclusively opines that: ‘People will always source physical products from the internet so whilst these purchases are *cloud assisted* – assisted by cloud technologies - they would still take place regardless of the cloud. In contrast, *a cloud dependent* cybercrime would include, for example, some forms of data-theft, especially the theft of, or manipulation of a complete cloud. Take away the cloud aspect and the crime disappears. In between are *cloud enabled* cybercrimes; mass scam spams, for example, would (in estimation) reduce from 10 billion every 10 seconds to 10 million every 10 minutes if the cloud technologies were removed’[26]. There is no silver bullet solution to cloud crimes as new innovations grow and are implemented in the CC. The same is true of CC threats, vulnerabilities and their outcome as risks.

CSA TOP THREATS	2010	2013	2016 The Treacherous 12	2019 *Egregious Eleven*
1	Abuse and nefarious use of cloud computing	Data breaches	Data breaches	Data Breaches (1)
2	Insecure application programming interfaces	Data loss	Weak identity, credential and Access management	Misconfiguration and Inadequate Change Control
3	Malicious insiders	Account hijacking	Insecure APIs	Lack of Cloud Security Architecture and Strategy
4	Shared technology vulnerabilities	Insecure APIs	System and Application Vulnerabilities	Insufficient Identity, Credential, Access and Key Management
5	Data loss/Leakage	Denial of Service	Account hijacking	Account Hijacking (5)
6	Account, Service & Traffic hijacking	Malicious Insiders	Malicious Insiders	Insider Threat (6)
7	Unknown Risk Profile	Abuse of Cloud Services	Advanced Persistent Threats (APTs)	Insecure Interfaces and APIs (3)
8	--	Insufficient Due Diligence	Data loss	Weak Control Plane
9	--	Shared Technology Issues	Insufficient Due Diligence	Metastructure and Applistructure Failures
10	--	--	Abuse and Nefarious Use of Cloud Services	Limited Cloud Usage Visibility
11	--	--	Denial of service	Abuse and Nefarious Use of Cloud Services (10)
12	--	--	Shared technology vulnerabilities	--

Table 4 CSA top threats to cloud computing

The relevant contemporary literature is quite rich in respect of analyzing countermeasures and also solutions of these cyber issues as evident in the contributions of Mithunzi et al. [27], Kumar and Goyal [28]Senyo et al, [29], De Donno et al. [30], Singh et al. [31], Fernandes et al. [32],Modi et al**. [33],** Coppolino et al .[34],Khalil et al.[35], Latif et al. [36], Zissis andLekkas [37], Asvija et al. [38], Litchfield and. Shahzad [39], Zafar F. et al, [40]. Recently, Mithunzi et al. (2019) have proposed a holistic view to facilitate 'comprehensive security analysis and the development of robust cloud security countermeasure'. In **Table 4** the Cloud Security Alliance (CSA) lists of cloud threats which give the concerned an awareness of the prevailing the threats and changes in their rankings in the cloud environment [28] [41]. The 2019 Final Report of the CSA ranked the threats in order of significance per survey results (with applicable previous rankings). The ranking is based on rating of the 241 industry experts in regard to the salient threats, risks and vulnerabilities in cloud computing. CSA reports that 'new, highly rated items in the survey are more nuanced and suggest a maturation of the consumer's understanding of the cloud. These issues are inherently specific to the cloud and thus indicate a technology landscape where consumers are actively considering cloud migration. Such topics refer to potential control plane weaknesses, metastructure and applistructure failures and limited cloud visibility. This new emphasis is markedly different from more generic threats, risks and vulnerabilities (i.e. data loss, denial of service) that featured more strongly in previous *Top Threats* reports' [**41**]. Before an overview of the cloud threats is profiled in the present paper, it needs to be said that threats can be categorized into policy-related, technical and legal issues along with miscellaneous issues associated with the deployment of the Cloud –based services'[42].In **Figure 4** Deshpande and others (2019) exhibit it.

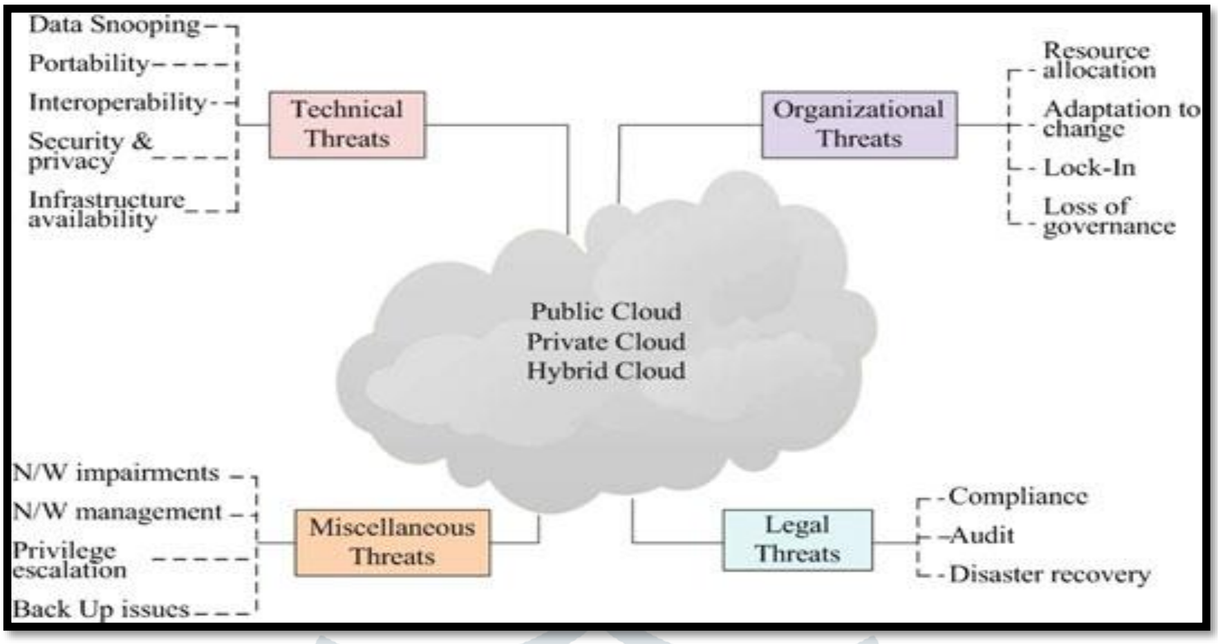


Figure 4 Threat classification of Cloud: a deployment model scenario

In the following **Table 5** Deshpande and others [42] also present security threats with deployment models such as public cloud, private cloud and Hybrid Cloud.

DEPLOYMENT MODEL	ASSOCIATED THREATS
Public Cloud	**1. Segregation failure. 2 Malevolent insider. 3. Data snooping and Seepage. 4. Distributed denial of services (DDoS). 5. Backup- and storage-related issues.**
Private Cloud	**1. Segregation failure. 2. Malicious probing or scanning. 3. Network impairments. 4. Backup- and storage-related issues.**
Hybrid Cloud	**1. Segregation failure. 2. Distributed denial of services (DDoS). 3 Social engineering attacks.**

Table 5 Security threats with Cloud deployment models

Parikh and others [43]give an outline of the architectural issues embedded in IaaS, PaaS, and SaaS, and also suggest their remediation in the following **Table 6.**

	Issues	Solutions
Iaas	1. Unauthorized control over confidential data. 2. Data theft by malicious user. 3. Monitoring VMs from the host machine. 4.Monitoring the VM another from another VM.	1. Monitoring network. 2. Implementing the Firewall. 3. Segmentation of network.
PaaS	1. Absence of secured soft ware progress by the CSP. 2. Recover and back up due to system failure or outage. 3. Inadequate provisions in the SLA. 4. Legacy applications provided by the vendors.	1. Encapsulation of access control policies. 2. Trusted Computing Base (TCB) as collection of secure files acts as an added layer over the OS. 3. Authorization enforcement for admission requests.
SaaS	1. Inability to maintain compliance standards regularly. 2. Inability to assess CSP's operations. 3. Inefficient authorization and authentication. 4. Data losses and data breaches.	1. Encryption of user data. 2. Recovery Facilities. 3. Email security from spams and malware. 4. Backup of user data on system outage.

Table 6 CC Architectural Issues and their Solutions

Table 7 shows group based CC threats summarized from the survey results of Maniah et al. (2019) to illuminate the relationship between types of threats with cloud service resources in the cloud computing[44]. They enumerate four types of group based CC threats such as threats to applications, threats to data, threats to infrastructure, and threats to general CC services. It also names the type of threats linked to each group based threats in the CC. **Table 8** offers a general overview of different security threats, attacks, vulnerabilities and their preventions at basic, network and application layers of the CC [42][45].The cloud environment has vast amount of distributed resources which enable the CSP to process the data. And this exposes security threats for which it is needed to control and mitigate unauthorized access to the user's data over the network [45].

No	Group of Threats	Type of Threats
1	Threats to Applications (e.g., attacks on software and virtualization)	1. Bugs in large distributed systems. 2. Software Licensing. 3. The feat of unauthorized access. 4. Attacks against virtualization. 5. API-level attacks against cloud services. 6. Account or service hijacking .7. Costumer data manipulation. 8. Eaves dropping. 9. Hypervisor viruses. 10. Using suspicious software .10. Trusted transaction. 11. Insecure APIs. 12. Injection and XSS Attack.
2.	Threats to Data (e.g., authorization to analyze data, disturbances due to data transfer, incorrect data handling, data manipulation, corruption of data)	1. Data/Vendor Lock-In .2.Data Confidentiality &Auditability. 3. Data Transfer Bottlenecks .4. Data corruption. 5. Data breaches. 6. Data scavenging. 7. Data leakage. 8. Insecure VM migration. 9. Improper virtual machine management. 10. Legal interception point. 10. Smart phone data slinging.11. Roll back attack. 12. Data manipulation. 13. Data loss or Leakage.
3.	Threats to Infrastructure (e.g. failure/damage to the infrastructure including mutitenancy)	1. Scalable storage. 2. Infrastructure failure. 3. Multi-tenancy. 4. VM escape. 5. VM Hopping and Malicious VM creation. 6. Insecure VM migration. 7. Sniffing/spoofing virtual networks. 8. Shared technology vulnerabilities. 9. TCP/ Session Hijacking.
4.	Threats to Cloud Services in General	1. Availability of Services. 2. Performance Unpredictability. 3. Scaling Quickly. 4. Reputation Fate Sharing. 5. Difficulty in detecting problems. 6. Old attacks with new implications. 7. Loss of Control. 8. Trust Chain in Clouds. 9. Abuse use of cloud computational resources. 10. Denial of service. 11. Elevation of Privilege. 12. Repudiation. 13. Wrapping attack. 14. Violation of SLAs. 15. Cloud security attacks. 16. Weak Service Level Agreements (SLAs)

Table 7 Group of Threats and associated type of Threats

10Nature of Threats	Security Threats Nomenclature	Description	Vulnerability	Prevention
BASIC SECURITY	SQL injection attack	A malicious code is placed in standard SQL code	Unauthorized access to a database by the hackers	May be avoided by the use of dynamically generated SQL in the code and filtering of user input
	Cross site scripting (XSS) attack (Web2.0/SaaS Security)	A malicious script is injected into Web content	Website content may be modifiedby the hackers	Active content filtering, Content based data leakage prevention technique, Web application vulnerability detection technique
	Man inmiddle attack(MIM)	Intruder tries to tap the conversion between sender and receiver	Important data /information maybe available to the intruder	Robust encryption tools like Dsniff, Cain, Ettercap, Wsniff and Airjackmay be used for prevention
NETWORK SECURITY	DNS attack	Intruder may change the domain name request by changing the internal mapping of the users	Users may be diverted to some other evil Cloud location otherthan the intended one	Domain name system securityextensions (DNSSEC) may reduce the effect of DNS attack
	Sniffer attack	Intruder may capture the data packet flow in a network	Intruder may record, read and trace the user's vital information	ARP based sniffing detection platform and round trip time (RTT) can be used to detect and prevent the sniffing attack
	IP address reuse attack	Intruder may take advantage of switchover time/cache clearing time of an IP address in DNS	Intruder may access the data of a user as the IP address is still exists in DNS cache	A fixed time lag definition of ideal time of an IP may prevent this vulnerability
	Prefix Hijacking	Wrong announcement of an IP address related with a system is made	Data leakage is possible due to wrong routing of the information	Border gateway protocol with autonomous IDS may prevent it
	Fragmentation attack	Malicious insider(user) or an outsider may generate this attack	This attack use different IP datagram fragments to mask their TCP packets from targets IP filtering mechanism	A multilevel IDS and log management in the Cloud may prevent these attacks
	Deep packet inspection	Malicious insider (user)	Malicious user may analyze the internal or external network and acquire the network information	
	Active and passive eaves-dropping	Malicious insiders and network users	Intruder may get network information and prevent the authentic packets to reach its destination	
APPLICATION LAYER SECURITY	Denial of service attack	The usage of Cloud network may get unusable due to redundant and continuous packet flooding	Downgraded network services to the authorized user, Increases the bandwidth usage	Separate IDS for each Cloud may prevent this attack
	Cookie Poisoning	Changing or modifying the contents of cookies to impersonate an authorizeduser	Intruder may get unauthorized access to a web page or anapplication of the authorized user	A regular cookie cleanup and encryption of cookie data may prevent this vulnerability
	CaptchaBreaking	Spammers may break the Captcha	Intruder may spam and over exhaust the network resources	A secure speech and text encryption mechanism may prevent this attack by bots

Table 8 Security threats and their solutions in Cloud Computing

In this regard it should be noted, as Hashizume and others say, there exists important relationships and dependencies between the cloud servicing models. Since both PaaS and SaaS are hosted on the top of the IaaS, then any breach in the IaaS will affect both PaaS and SaaS . This holds true on the other way round. Further, 'we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies, any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks' [46].

II.CLOUD COMPUTING SECURITY

II.RISKS AND COUNTER MEASURES

It has already been stated that risk refers to 'the ability of a threat to exploit vulnerabilities and thereby causing harm to the system. Risk occurs when threat and vulnerability overlap. It is the prospect of a threat to materialize' [18]. Stated otherwise, risk is a probability of occurrence of an event that may interfere with the achievement of desired goals. In both cloud and non-cloud technology systems the nature of security (i.e. security, reliability, and performance) are similar. But ‘the degree of risk the degree of risk and its profile varies if Cloud solutions are adopted depending on the impact of risk events (residual and natural) associated with the CSP’. In **Table 9** there is an over-all view of risks and their mitigation [47].

CLASSIFICATION OF THE RISK IN CLOUD PARADIGM

Classification	Nomenclature/ Severity of Risk	Vulnerability	Effect on	Mitigation policy
Policy related Risk	1. Lock-In/ High	Lack of standard technologies and solutions	Credibility of CSP, personal data of users, service quality	Risk reassignment
	2. Failure of governance/High	Undefined roles, responsibilities, and ownership	Customers trust, employee loyalty and CSP reputation	Risk reassignment
	3. Compliance challenges/High	Unavailability of audit/certification to the customers	Service limits due to compliance issues	Risk acceptance
	4. Loss of business due tocotenant activities/Medium	Poor resource isolation	Service delivery and personal data	Risk avoidance
	5. Service termination/Medium	Less transparency in terms of use	Service delivery	Risk avoidance
	6. CSP acquisition/Medium	Inter Cloud application dependency	Intellectual property, personal data	Risk approval
Technical and Security risk	7. Under or over provisioning of the resources/Medium	Inaccurate estimate of resource usage	Access control, authentication and authorization (AAA)	Risk alleviation
	8. Segregation failure/High	Hypervisor vulnerabilities	QoS due to multi-tenancy	Risk avoidance
	9. Malevolent insider/High	Inadequate security procedures	Integrity and availability of all the data	Risk avoidance
	10. Availability of Infrastructure/Medium	Misconfiguration	Real time services	Risk alleviation
	11. Snooping of the data/high	AAA failure	Security attacks such as sniffing, eavesdropping, man-in-middle, side channel and reply attacks may be dominant	Risk avoidance
	12. Data seepage/High	AAA and communication encryption failure	transfer of data between CP and user	Risk reassignment
	13. ineffective deletion of the data/Medium	susceptible media cleansing	Critical data may be lost	Risk alleviation
	14. distributed denial of service (DDoS)/High	Misconfiguration	CSP management interface	Risk avoidance
	15. loss of encryption keys/High	Poor key generation mechanism	Credentials and personal data may be lost	Risk reassignment
	16. Malicious probing or scanning/Medium	Internal network probing may occur	User trust.	Risk avoidance
	17. Compromise service engine/Medium	Lack of resource isolation	Service delivery	Risk avoidance
	18. Conflict involving customer consolidation measures and Cloud environment/Medium	Conflicting SLA clauses and transparency in operation	The roles and responsibilities of CSP and the customers	Risk reassignment
Legal Risk	19. Subpoena and E-discovery/Medium	Lack of resource isolation and transparency in data storage	Users critical data, trust	Risk approval
	20. Change of jurisdiction/High	information on jurisdictions	Users data held at multiple jurisdiction may put it in a high risk state	Risk approval
	21. Data protection/High	Lack of transparency in location of data storage	Company reputation may be at stake	Risk avoidance
	22. License issues/Medium	Lack of transparency in terms of use	Certification and service delivery	Risk approval

Miscellaneous risk	23. Network Impairments/High	Misconfiguration, system or OS related issues, poor resource isolation	Potentially thousands of customers were affected at the same time	Risk avoidance
	24. Network Management/High	Network congestion, misconnection and non optimum use	Service latency will be disturbed	Risk reassignment
	25. Network traffic modification/Medium	No control over vulnerability assessment	Data retrieval	Risk reassignment
	26. Privilege Escalation/Medium	AAA mishap	Users personal data	Risk avoidance
	27. Social engineering attacks/Low	Lack security awareness and resource isolation	CRP trust and users personal data	Risk avoidance
	28. Backup related issues/Medium	Lost or stolen backup	Company reputation	Risk reassignment
	29Unauthorized access to the system/Medium	Inadequate physical security measures	Company reputation, users trust, sensitive data	Risk avoidance
	30. Theft of PCs/Medium	Inadequate physical security measures	Company reputation, users trust, sensitive data	Risk avoidance
	31. Natural Disaster/Medium	--	Data storage	Risk avoidance

Table 9 Overview of Risks and their Mitigations

While Deshpande and others provide an overview of risks from a broader perspective, Latif and others [48] present, on the basis of their critical analysis of 31 studies out of 100 papers, a important list of CC risks from the viewpoints of both the Cloud Provider (CP) and the Cloud Consumer (CC). In **Table 10**. Deshpande and others tracethe risks as inherent characteristics and due to deployment strategy. They recommend for minimizing the risks by employing strategies like risk reassignment, risk alleviation, risk approval and risk avoidance[47]. In contrast Latif and others consider risks from specific aspects suchas data security and privacy, technology etc. They suggest not complete mitigation but only to 'some extent' [38].

III. INCREASING CHALLENGES OR DEFICITS IN COUNTERMEASURES? UNCERTAINTY OF CLOUD COMPUTING

It is quite evident from the preceding analysis that, generally speaking, CC challenges and security controls go a long way to protect 'the computing system and its stored data from any damage or harm'. In the contemporary digital economy and society, information assets such as data, information, hardware, software and networks require safety measure for their more often than not invaded by cyber threats, attacks, vulnerabilities and risks. But, unfortunately, technical solutions or implementation of remedial counter measures are often not adequate. For instance, if the firewalls are not managed properly or the users cannot operate it properly, then the meaning of control is lost **[49]**. von Solms emphasises the need for information security in terms of three waves. In the first wave—the technical wave-- lasting up to 1980s, technical approach was deemed alright. In the second wave -- the management wave -- from the early 1980s to mid-1990s there was the increased realization of ensuring information security by the management in the organization set-up. The later years of the 1990s the third wave—institutional wave—were characterized by the acceptance of best practices codes of practice , and security certification marking the rise of dynamic and continuous cultivation of information security as part of culture including and emphasis on security awareness[50]. Since then the importance of the theme of cyber safety continues to reign among the concerned, as reflected in the literature especially in the light of information and cyber security cultural analyses[51][52][53][54][55][56][57][58][59][**60**][61]. It has been rightly argued that security issues in the cyber world require coordinated and directed effort at all levels. ranging from all stake holders including the individual –the computer owner – when it has become basically his responsibility to manage the cyber risks for his systems and devices in view of lack of pro-active or substantive safety defences from the government or government bodies [54] **[**[62]. The advent of the Information Revolution,

	RISKS	SECURITY MEASURES
DATA SECURITY AND PRIVACY	**Ensure availability of customer's data in Cloud. (CP)**	**Specific security measures have been taken by CSP to prevent outages and attacks.**
	Risks related to data security and privacy. (CP), (CC)	**1. To mitigate these risks is using APIs to implement a robust access control, using encryption to protect data traffic. 2. Analyze that data is protected during design time, as during runtime. 3. Provide effective mechanisms for key generation, storage, and destruction of data.**
	Preventing unauthorized access to customer's data in the cloud. (CP), (CC)	**Can be resolved by implementing Management, authentication and authorization techniques on both customer and provider's**

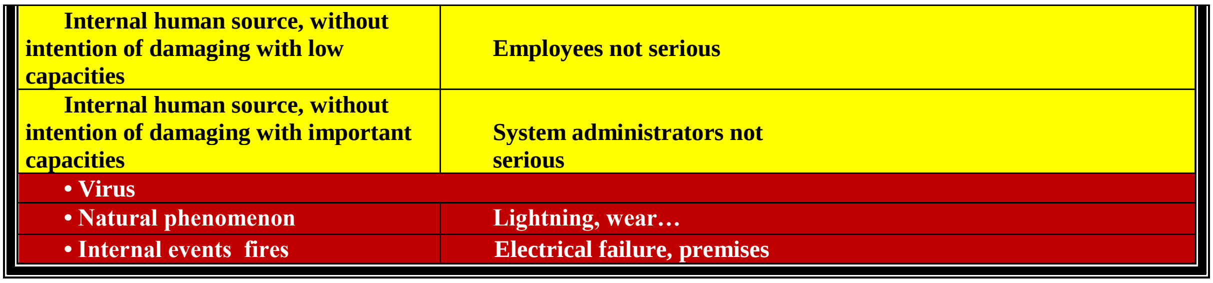
		sides.
	Risks related to multi- tenancy .(CP)	CSP should use effective encryption methods to guarantee data isolation between clients.
	Risks related to data deletion .(CP)	The provider should define policies to establish procedures for the destruction of persistent media before throwing it out.
TECHNOLOGY	Lack of standardized technology in the cloud computing system. (CC)	The customer should ensure if the provider uses standardized technology and it should be mentioned in its initial contract.
	Compatibility issue between cloud and IT systems in customer's organization.(CC)	The solution is to use the hybrid cloud, which is capable of handling much of these compatibility issues.
ORGANIZATIONAL	Risks related to Resource Planning, Change Management. (CC)	Involves stakeholders in cloud adoption procedures.
	Risks related security management. (CC)	Re-evaluate existing security standards before cloud adoption.
PHYSICAL SECURITY	The physical security of a cloud provider's data centers composed of servers, storage and network devices. (CP)	Cloud providers must have certain policies and procedures in place to prevent physical security breaches these includes physical location security like alarms, CCTV cameras etc.
COMPLIANCE	Enforce regulatory obligations in a cloud environment. (CP)	1. CSP must abide by all the regulations within a country, regarding. cloud security. These regulations include HIPPA, FISMA. 2. CSP has to contend with the Legal Systems under different Jurisdictions with not so much of visibility as to where the Data resides and how it is routed by passing through different Legal Jurisdictions.
	Business Continuity and Disaster Recovery. (CP)	Recommends replicating data across multiple infrastructures to avoid vulnerabilities in the event of a major failure.

Table 10 CC and CP Risks and suggested Countermeasures

precipitated by the ICTs, have brought to the fore privacy and security issues and, so naturally, 'more significantly the concept of cyber security'[63].

It has beenasserted that 100% security is not possible [64] *vis a vis* onslaughts against attacks on the computer technology assets from hackers in the cyberspace. Huang and Pearlson, two cyber security specialists at MIT instructively go on to say that 'Even the most advancedtechnological security cannot protect an organization from a cyber breach if the people in the organization are not careful and protective. ... In today's cyber world, it only takes one employee clicking on a phishing email to provide an attacker with an entry point into the systems running a business. Once inside, an attacker can lock up critical information, as seen in the WannaCry virus, or bring down critical infrastructure as in the Ukraine, when the Petra attack took nuclear radiation monitoring offline, or more commonly, result in a data breach incident'**[**65]. Technological security remains incomplete simple because technology is after all 'dumb and deterministic' whereas humans are 'creative problem solver' [66].**ENISA**, in its report (2018), focuses attention to the human aspects of cybersecurity and how it bears on different facets of human behaviours based on lessons of behavioural sciences that take humans as its main focalpoint. It championed the point that "The insight that humans are an integral part of delivering cybersecurity is not new, but only over the past 20 years has there been a significant body of social science research that looks at cybersecurity as a socio-technical problem and develops guidance on how to manage that problem effectively. The socio-technical perspective includes the actions (and decisions) of policy makers and security professionals; systems designers, developers and requirements engineers; and end users' [**67**].It is quite appropriate to mention here that it is precisely certain human errors that cause CC threats. to which Belbergui et al. [68] explicitly draw their attentionin the following **Figure 5**.Cyber security culture(CSC), as **ENISA** (2017) conceptualizes,

TYPES OF THREAT SOURCES	EXAMPLES
• Human sources	
- Internal attacks	
Malicious internal human source with low capacities	Personal
Malicious internal human source with significant capabilities	The IT manager
- External attacks	
Malicious internal human source with low capacities	Housekeeping staff
Malicious external human source with significant capabilities	Competitors Computer maintenance staff



Internal human source, without intention of damaging with low capacities	Employees not serious
Internal human source, without intention of damaging with important capacities	System administrators not serious
• Virus	
• Natural phenomenon	Lightning, wear…
• Internal events fires	Electrical failure, premises

Figure 5 Threat sources in a cloud computing

'refers to the *knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity* and how they manifest in people's behaviour with information technologies. CSC is about making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions'. Cyber security policies are rules rather than guidelines. CSC changes 'in mindset, fosters security awareness and risk perception and maintains a close organisational culture, rather than attempting to coerce secure behaviour' [69]. Huang and Pearlson states that organizational cybersecurity culture as "*the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber attacks*' and in the cybersecurity, being more thana technical issue,the 'ultimate goal for manager is to drive cybersecurebehaviors' among all organizational employees. The **Figure 6** illustrates their cultural frame work [65]. The counterpart of CSC is Information Security Culture (ISC) is defined by AlHogail and Mirza as the 'collection of perceptions, attitudes,value, assumptions and knowledge that guides how things are done in organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behaviour in a way that preserving the information security becomes a second nature' **[**70].

It should also be noted here that it is not true that no one refers to the human, to behavioural security measure to protect the cloud environment. Mell right argues that present security issues new use of 'the existing general purpose security controls'[71]. For Example, Amron and others talk of 'human readiness' and management's support and ability [72], Mithunzi and others include 'human factor' as part trust issue in their general view of cloud computing[27], Singh and Chatterjee take in 'human aspect' as part of trust management [**73],** Quedraogo and others refer to employees' accidental or malicious tampering or leakage of data[74**],** Hashizume et al. point to such vulnerabilities as, lack of employee screening and poor hiring, Lack of customer background checks, and lack of security education [46], Caulking notes the 'behavioral side of the education and training within the cyber domain' and stresses the focus on 'human side' of cyber such as insider threats, policy and strategy, training and education, ethics, legal issues, users remodelling, and other related issues [75],

Wiley et al. underscore the inadequacy of only technical solutions' champions a 'strong security culture' because 'employees from organisations with a better security culture were more likely to have the knowledge, attitudes, and behaviours in accordance with information security policies and procedures required to maintain good information security in the organisation'[76], and Sultan and Bunt-Kokhuis argues for 'a cultural overhaul of theway' the IT vendors used to do their business [77], and, finally, Govender et al. remark that 'in effect,developing and enhancing the socially relevant factors creates a stronger foundation for success of the technical factors'[78].

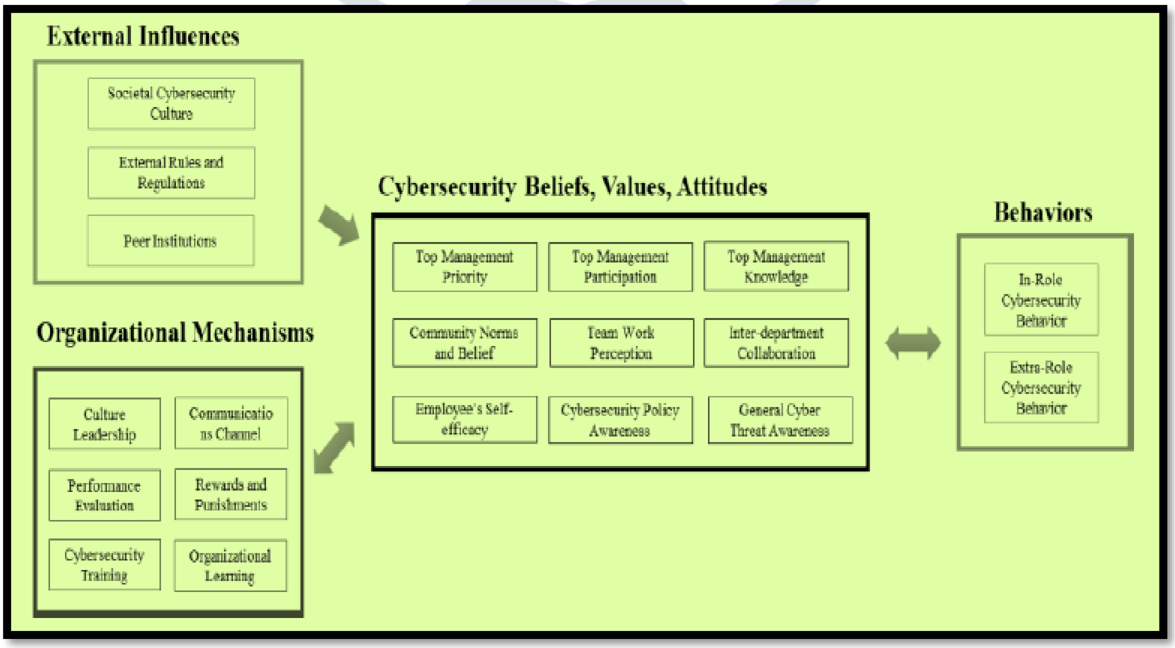
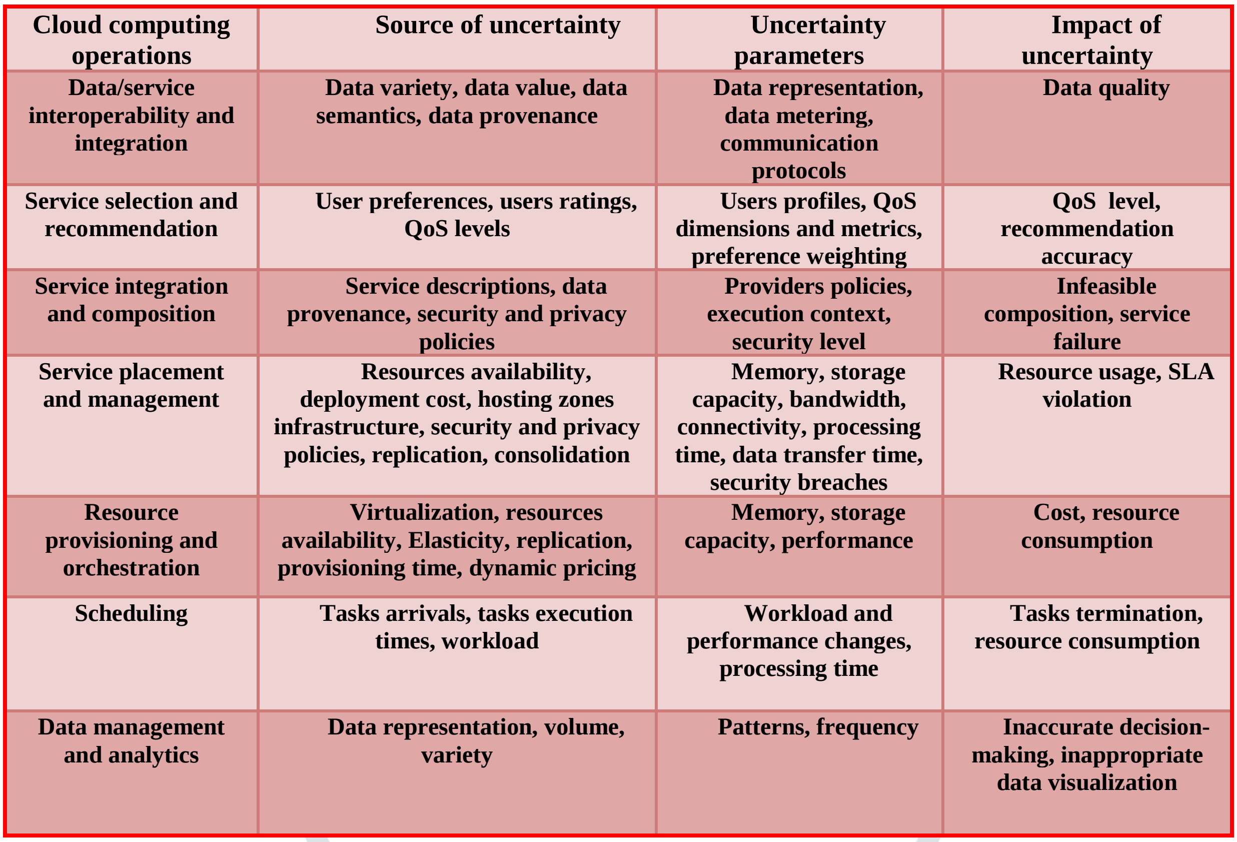

External Influences
Societal Cybersecurity Culture
External Rules and Regulations
Peer Institutions
Organizational Mechanisms
Culture Leadership
Communications Channel
Performance Evaluation
Rewards and Punishments
Cybersecurity Training
Organizational Learning
Cybersecurity Beliefs, Values, Attitudes
Top Management Priority
Top Management Participation
Top Management Knowledge
Community Norms and Belief
Team Work Perception
Inter-department Collaboration
Employee's Self-efficacy
Cybersecurity Policy Awareness
General Cyber Threat Awareness
Behaviors
In-Role Cybersecurity Behavior
Extra-Role Cybersecurity Behavior

Figure 6 Organizational Cybersecurity Culture Model



Cloud computing operations	Source of uncertainty	Uncertainty parameters	Impact of uncertainty
Data/service interoperability and integration	Data variety, data value, data semantics, data provenance	Data representation, data metering, communication protocols	Data quality
Service selection and recommendation	User preferences, users ratings, QoS levels	Users profiles, QoS dimensions and metrics, preference weighting	QoS level, recommendation accuracy
Service integration and composition	Service descriptions, data provenance, security and privacy policies	Providers policies, execution context, security level	Infeasible composition, service failure
Service placement and management	Resources availability, deployment cost, hosting zones infrastructure, security and privacy policies, replication, consolidation	Memory, storage capacity, bandwidth, connectivity, processing time, data transfer time, security breaches	Resource usage, SLA violation
Resource provisioning and orchestration	Virtualization, resources availability, Elasticity, replication, provisioning time, dynamic pricing	Memory, storage capacity, performance	Cost, resource consumption
Scheduling	Tasks arrivals, tasks execution times, workload	Workload and performance changes, processing time	Tasks termination, resource consumption
Data management and analytics	Data representation, volume, variety	Patterns, frequency	Inaccurate decision-making, inappropriate data visualization

Figure 7 Sources and Impact of Uncertainty on Cloud Computing

All this boils down to the fact that in preventing or mitigating cloud threats and risks the important requirement is to approach security problems in the cloud environment from an interdisciplinary perspective based on ‘several disciplines, namely information systems, computer science, computer engineering, finance, accountingand so on’ [29**].** Yu et al. strengthen the argument further: ‘Cloud computing security research resides in an interdisciplinary area that includes technological, behavioural, managerial and social dimensions’ [79]. Singh et al. include, in their classification of cloud computing security issues,both ‘ human factors and forensics value’ [80]. It is now quite understandable in the preceding context why Hasizhume et al raises the issue of uncertainty surrounding CC security [46]. In fact, in an excellent contribution,Menzi et al. characterized CC as ‘the uncertain cloud’. The **Figure7** describes it in all its dimensions [**81**].

V. CONCLUDING REMARKS: CLOUD COMPUTING IN THE LATE MODERN RISK SOCIETY

The worldwide popularity in expansion of CC is unquestionable in view of enormous spending on cloud services attests to the ‘the magnificence huge movement in the field of information technology business. Nowadays, business enterprises seek to reshape their business models to gain benefit from new paradigm and reduce the cost’ [82].According to Gartner forecasting, ‘the worldwide public cloud services market’is projected to grow 17.5 percent in 2019 to total US$214.3 billion, up from US $182.4 billion in 2018. Accordingly to worldwide public cloud service revenue forecast is expected to grow from 182.4 to 249.8 in 2020 andwill reach US$ 331.2 in 2022 in billion US Dollars [83]. Even in India , according to a survey of Goggle Trends, the progress of CC in India was faster than anywhere else in a list of 10 countries ranked in surfing CC. Garter’s estimated SaaS market in India at US$27 million in 2007[84]. CC market in India increased to 1.3 billion dollars in 2017- ‘a 38% year-on-year growth’ and is projected to reach 4.1 billion dollars by 2020.Gratner estimates that India’s public cloud services (in millions of US Dollars) will be 1,187 in 2017, 3,169 in 2019 and 4,104 in 2020[85]. Cloud spending is estimated to grow at 30% per annum to hit 7.1-7.2 billion in US Dollars in 2022 [86] The reasons for this explosive expansion of CC in the world or in India is not far to seek.

It is the benefits which CC offers to all, both organizations and individual consumers. Key benefits are indeed many that **‘**include reduced capital and operational cost, improved flexibility,on-demand scalability, easier and quicker application deployment, ease of use, and availability of vast cloudresources for every kind of application or use. Many applications, including e-mail, office document creation,and much data storage continue to move into the clouds to reap the benefits of this new paradigm in IT. Cloud computing frees users and businesses from the limitations of local computing resources and allows them to access the vast computational resources and computation power out in the cloud. For users to make use of cloud resources from anywhere in the world at any time, all that is needed is an Internet connection and a Web browser. The cloud lets the users run even computationally intensive or storage-intensive applications, as all of their computing and storage needs are sourced from the cloud ... Cloud applications can be deployed instantly and simultaneously to thousands of users in different locations around the world, and can be regularly updated easily. Further, as clouds provide improved business continuity and data safety, they are particularly attractive to small- and medium-size enterprises, as well as enterprises in disaster- prone areas. Startups and application developers can use computing clouds to try their ideas without having to invest in their own infrastructure’ [15]. However, expanding investment on and extensive use of CC does not mean that CC is without limitations, especially threats, vulnerabilities or risks, as evident in the concerned literature or as empirically evidenced by relevant statistics and concrete organizational experiences.

For instance, from 2019 to 2022, the top 10 most targeted industries for cyber attack are healthcare, manufacturing, financial services, government, transportation, retail, oil and gas/energy and utilities, media and entertainment, legal, and education.In 2018, the most common cyber attacks against companies were phishing (37%), network intrusion (30%), inadvertent disclosure (12%), stolen/lost device or records (10%), and system misconfiguration (4%)..In 2013 Yahoo experienced biggest data breach of all time affecting 3 billion accounts. Between 2014 and 2018, this figure is 500 million for Marriott. DDoS attack will reach 14.5 million by 2022. Hacking tools and kits for all types of cybercrimes are available online for only US$ 1. Finally, the global cybercrime economy makes a profit about US$ 1.5 trillion annually. 'Ironic as it may be, every technological advancement tends to result in an increase in cyberattackincidence. Innovations like IoT, mobile payments, and cloud computing, unfortunately, have given birth to new sophisticated cybercrime activities [87]. It took in average 206 days in 2019 to identify a data breach, while hackers attack 39 seconds, total number of attacks being on average 2,244 times a day. Most business leaders (68%) feel that their cybersecurity risks are increasing. Emails delivered 94% of malware. It is stated that 34% of data breaches involved internal actors and that 69% of organizations don't believe the threats they're seeing can be blocked by their anti-virus software. Further, 53% of companies had over 1,000 sensitive files open to every employee and 15% of companies found 1,000,000+ files open to every employee [88]. A few examples of different threats, vulnerabilities or risks as experienced by different organizations and individuals may also be cited from the CSA's Report on Top *Threats to Cloud Computing The Egregious Eleven* (2019). In 2019, Voipo, a telecoms company that provides Voice over Internet Protocol (VoIP) services, experienced a data breach in total of ' 7 million call logs, 6 million text messages and other internal documents containing unencrypted passwords that— if used—could allow an attacker to gain deep access to the company's systems' in 2018.In respect of vulnerability and threat embedded in misconfiguration and inadequate change control, Level One Robotics, an engineering company specializing in automation process and assembly, in 2018' exposed highly sensitive proprietary information belonging to more than 100 manufacturing companies, including Volkswagen, Chrysler, Ford, Toyota, General Motors, Tesla and ThyssenKrupp'.Due to non-implementation of appropriate security structure and strategy, a technology and cloud giant Accenture in 2017 inadvertently left unsecured four Amazon S3 buckets containing 'hundreds of gigabytes of data for the company's enterprise cloud offering, which the company said provides support to the majority of the Fortune 100 companies. The data could bedownloaded without a password by anyone who knew the servers' web addresses'. Concerning malicious insider, the Report says that in 2018 an insider swindled US$1.8 billion from 'Punjab National Bank in India. An employee at that bank used unauthorized access to an extremely sensitive password in the SWIFT interbank transaction system to release funds in a highly complex fraudulenttransactional chain schemed up by a diamond merchant to buy rough stones from suppliers'. In respect of insecure interfaces (UIs) and APIs the CSA Report says that 'Facebook announced a significant data breach affecting more than 50 million accounts on Sept.28, 2018. Reportedly, credential theft vulnerability was introduced into Facebook code in Julyof 2017, more than a year earlier. The company admitted it didn't know what information wasstolen, nor how many other user accounts were compromised as a result of the breach' [41].

Without multiplying the examples any more, it is crystal clear that CC, however popular and widely used, is intrinsically liable to be affected by security issues 'because of the complexity of the cloud scenario (e.g., dynamic distribution, virtualization, and multitenancy), because data or computations might be sensitive, and should be protected even from the provider's eyes, or because providers might be not fully trustworthy and their – possibly lazy or malicious – behavior should be controlled' [89]. It is thus not extraordinary fact that even though adoption of CC continues to surge, security concerns show no sign of abatement according to 2018 Cloud Security Report. It reports that 9 out of 10 cybersecurity professionals remain concerned about cloud security, up 11% from last year's cloud security survey. The top three cloud security challenges are protecting against data loss and leakage 67%, threats to data privacy 61%, and breaches of confidentiality 53 percent%. The single biggest threat to cloud security (62%) is misconfiguration of the cloud platforms, followed by unauthorized access through misuse of employee credentials and improper access controls (55%), insecure interfaces/APIs 50%., Hijacking of accounts, services or traffic (47%), External sharing of data (39%), Foreign state sponsored cyberattacks (33%), malicious insiders (30%), Malware/ransomware (26%), and Denial of service attacks (22%) [90]. ENISA reminds the enterprises the need to 'understand and evaluate all the risk factors involved with migration, provisioning, and adopting cloud services' in view the changes in the threat landscape in view of constant cyber attacks and breaches. As it warns: 'The enterprise is expected to stay up to date and protect against the latest threats, risks, and vulnerabilities. Ransomware attacks like WannaCry affected over 250,000 computers in 2017. Additionally, Bad Rabbit, Petya, and Not Petya also stormed the industry in 2017. Distributed-Denial-of-Service (DDOS) attacks like the one on Dyn DNS affected over 70 major online services. Other malware like the Mirai botnet in 2016 was responsible for multiple DDOS attacks on credible sites due to unsanitary security practices. Misconfigured cloud services such as the S3 bucket leaks by Alteryx7 that exposed information on 123 million Americans and one at Verizon8 impacting 6 million individuals. Meltdown and Spectre vulnerabilities exploited almost every modern processor to leaky data and passwords' [91].

In the light of the above analysis it is quite interesting, if not compelling, to state that the risks (inclusive of threats and vulnerabilities) of Cloud Computing closely parallel, are linked to and closely similar with, the discourse of Risk Society, initially formulated by Beck and Giddens, especially the former, two world acclaimed sociologists. Mythen rightly remarks that 'in the risk society narrative, seismic shiftsin the relationship between the natural and the social necessitate refreshed ways of conceptualising society'[92] in which CC is stated to be paradigmatic revolution dominating the domain of computing. Throughout the 1990s risk society discourse also 'offered 'a mew interdisciplinary paradigm linking the social and natural sciences' [93], was hailed as a kind of 'grand theory' or a 'diagnosis of the times' [94] and, at the same time stimulated various inter-disciplinary approaches and studies about role of risk in all its dimensions in the contemporary society [95][96][97]. Risk discourse covers such diverse fields as social theory, genetic engineering, cultural studies, medical sociology, communication,philosophy, biotechnology, cybernetics and utopianism, social inequality and class, politics and power, work and labour markets, economics, international relations, war and military, business and management, insurance, law and justice, criminology, terrorism, love and family, youth, media, technology andculture, science studies, environmental politics and global warming, globalization and cosmopolitanism and in brief 'Beck's Risk Society raises issues and concerns which are simplyirreducible to any one academic discipline' [98][99].Beck was not the first sociologist to use the term called risk society. It was an Israeli sociologist Yair Aharoni who in his book *The No-Risk Society* (1981) emphasizes the need for security for everyone and pleased for insurance against the risks which are 'side effects of industrialized society itself' [94].

In formulating his concept of risk society Beck was also influenced by François Ewald (1991) who considered that modem society a truly *insurance society*. Like any other technology including CC, the evolution of the risk society discourse was in several phases. Table 11 shows this [94].

BECK'S USE OF THE TERMS HAZARD AND RISK SINCE 1988 IN THE EVOLUTION OF THE RISK SOCIETY LANDSCAPE

Period	*Examples*	*Term*	*Cause*	*Possibility of avoiding harm*
Premodernsociety	Natural disasters, epidemics	Hazards	External causes	People are exposed to the events and cannot avoid them
Industrial society	Unemployment, accidents (traffic, work etc.)	Risks	Risks	People can (in principle) avoid or insure themselves against them
Risk society	Radioactive leaking, gene technology, holes in the ozone layer, Global warming, terrorism	Self-jeopardy, man-made disasters	Man-made	People are exposed to the events, cannot avoid them and cannot insure themselves against them

Table 11 Historical Evolution of the Risk Society

In the pre-modern humanity had not protection against non-man-made hazards which were not based on technological or economic decisions and thus attributed to external causes such as god, flood, drought etc. Although often used interchangeably, two terms hazards and risks were distinguished by Beck in 1988 when he defined risk as 'determinable, calculable uncertainties; modernity itself produced them in the form of foreseen or unforeseen secondary consequences, for which social responsibility is (or is not) taken through regulatory measures. They can be 'determined' by technical precautions, probability calculations, etc., but (and this is frequently not taken into account) also by social institutions for attribution, liability and by contingency plans' [94]. Non-man made hazards were limited in their range or scope. However with the coming of classical modernity theses non-made hazards were replaced by man-made risks which can be contained and were limited in their impact.The risk society truly arrives on the scene in the 1970s onwards when industrial society became transmuted into an actual risk society, when uncertainty- radioactive emissions, acid rain, gene technology, global warming etc- came back again. As Beck states, 'The entry into risk society occurs at the moment at which the manufactured risks undermine or annul the provident state's prevailing risk calculations. Those who ask for a operational criterion for this transition find their answer here: *the absence of private insurance protection.* ...Insurance protection (whether private or state-organized) had a twofold function from the perspective of social theory, namely, *neutralizing damage* and thereby *neutralizing fear*. To the extent that the expansion of risk outstrips insurance protection, the latter loses its function of neutralizing fear at boththe social and the political level, behind the still intact Potemkin façade of insurance protection. Free-floating fears are being set free' [94].The characteristics of first modernity, embracing industrial society, were (1) society as nation–state society, (2) Programmatic individualization, (3) Society as gainful employment society, (4) Nature is perceived as being separate from society, (5) Leaning on a scientifically defined concept of rationality illusive of instrumental control, and (6) Understanding and management of society's development based on functional differentiation. Stated otherwise, modern societies are nation state societies characterized by a programmatic individualization (institutionalized individualism), and gainful employment societies with full employment. These three were based on an instrumental view of nature, a scientifically defined concept of rationality, and the principle of functional differentiation. The features gradually weakened or dissolved withthe rise of five processes of change such as Multidimensional globalization, Radicalized/intensified individualization, Global environmental crisis, Gender revolution and The third industrial revolution. They mark the advent of second modernity or reflexive modernity in which society became gradually risk society [94]. This process involving the concept of reflexive modernization is described by Beck in these words; 'This precisely does *not* mean *reflection* (as the adjective 'reflexive' seems to suggest), but above all *self-confrontation.* The transition from the industrial to the risk epoch of modernity occurs intentionally, unseen, compulsively, in the course of a dynamic of modernisation which has made itself autonomous, on the pattern of *latent side-effects.* One can almost say that the constellations of risk society are created because the self-evident truths of industrial society (the consensus on progress, the abstraction from ecological consequences and hazards) dominate the thinking and behaviour of human beings and institutions. 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 modernisation processes which are blind and deaf to consequences and dangers. In total, and latently, these produce hazards which call into question - indeed abolish - the basis of industrial society' [100].**Table 12** show the differences between industrial society and risk society [94]. Risks irreversibly endangers the life of plants, animals and humans regardless of their territorial affiliation [101].

No,	**Beck's COMPARISON OF INDUSTRIAL SOCIETY WITH RISK SOCIETY IN TERMS OF ATTRIBUTES**	
1.	**Production of wealth**	**Production of risks**
2	**Elimination of scarcity/need**	**Elimination of risks**
3.	**Wealth distribution**	**Risk distribution**
4.	**An aim to achieve**	**An aim to avoid**
5.	**Combating reality**	**Combating possible futures**
6.	**Positive focus on the possibilities of the future**	**Negative focus on the future's potential disasters**
6.	**Being determines consciousness**	**Consciousness determines being (idealism)**

	(materialism)	
7.	Poverty	Anxiety
8.	I am hungry	I am afraid
9.	Us/them distinctions (rich/poor, American/Russian etc.)	Us/them distinctions are diluted and lose meaning
10.	Need is hierarchic	Smog is democratic
11.	The industrial process is apolitical	The industrial process is political (the sources of wealth are also the sources of pollution)

Table 12 Comparisonbetween Industrial Society and Risk Society

Risks are 'lurking everywhere'. The world is becoming a global risk society when 'we are becoming members of a 'global community of threats'. The threats are no longer the internal affairs of particular countries and a country cannot deal with the threats alone' [102].

What is the reason, or preeminent reason behind the rise of risk society? As Achterber summarises, 'their ultimate source is the development of science and technology. However, no longer are they just limited side effects of a technological development which seems on the whole benign and, at least in its particular manifestations, under control; no longer can they be considered the unavoidable price of a progress which brings material benefits to most people. The development of science and technology forms part of an autonomous process of modernization that leads inexorably in its later phases to what one may call a return of the repressed: pre-industrial hazards, the dangers of natural disasters, tend to lose their external character and become internal, manufactured and large-scale risks arising from our technological transformation of nature. They are internal because risk society has lost in its scientific and technological development any clear distinction between society (culture) and nature. They are large-scale because these internal risks, of which the ecological ones are heavily emphasized by Beck, are no longer limited in scale, neither geographically nor in time nor socially; by the same token they cannot be covered by any insurance. They are the result of modern technologies – nuclear, chemical, bio-industrial, genetic, etc. – which are actually out of (scientific and political) control even in their development, let alone in their so-called normal operation' [103]. Beck refers to 'the *failure* of techno-scientific rationality in the face of growing risks and threats from civilization'. He attributes it to the systematically grounded in the institutional and methodological approach to sciences in risks. Though incapable of reacting to these risks, they are prominently involved in the origin and growth of those very risks. He goes on to say that with techno-scientific concern with risks in the background "the engineering sciences' claim to a monopoly on rationality in risk perception is equivalent to the claim to infallibility of a Pope who has converted toLutheranism'. He adds that 'The first priority of techno-scientific curiosity is *utility for productivity*, and the hazards connected with it are considered only later and often not at all' [104]. The failure of techno-scientific rationality transcends national barriers. 'The concept of 'world risk society' however, draws attention to the limited controllability of dangers we have created for ourselves. The main question is how to take decisions under conditions of manufactured uncertainty, where not only is the knowledge base incomplete , but more and better knowledge often means more uncertainty' [105].

The basic contribution of the present paper is, *inter alia*, the suggestion that CC has become embedded in the industrial risk society. Although CC has its own set of risks, they are now part of and integral to the emergent risk society within and beyond national frontiers. The link is techno-scientific, as Beck would have called. Indeed there are many similarities and parallels between the two. Let me point out a few of them to make the point clear. For instance, first, the CC is widely accepted and deployed model for small, medium and large business concerns [106] in today's information capitalist society not only for delivering useful resources and services but also for making profit in the market. A 'new kind of capitalism' came into being in the industrial risk society with the breakdown of very idea of controllability, certainty or security, which was fundamental in the early modernity, and risks became a 'growing business' [105] [101]. Risks are becoming 'drivers of economic boom' and they have become a core component of 'developed capitalism' Risks continue to grow and are not completely eliminated. The approach to risk is preventive, but only a symbolic, politics and industry to eliminate proliferating risks' [101]. Second, as in the CC, risks in the risk society are 'no longer the dark side of opportunities, they are also *market opportunities.* As the risk society develops, so does the antagonism between those *afflicted* by risks and those who *profit* from them' He also says that 'there are fundamentally *two options* confronting each other in dealing with civilizational risks: removing causes in primary industrialization, or the secondary industrialization of consequences and symptoms, which tends to expand markets. To this point, the *second* route has been taken almost everywhere. It is cost-intensive, leaves the causes obscure and permits the transformation of mistakes and problems into market booms' [104]. Third, as in the CC where the concerned literature invariably deals with security issues and also frameworks of possible threats and their preventive prescriptions, in the industrial risk society security is also elusive. 'The promise of security grows with the risks and destruction and must be reaffirmed over and over againto an alert and critical public through cosmetic or real interventions in the techno-economic development' [104]. In a way, in various ways (viz. product development, advertising etc.) industries are constructing 'new problems and market new solutions' for fighting risks to sell security and in the process leading to increasing 'commoditisation of risk' [107], reminding one of the role of SLA (cloud service-level agreement)s in the CC. In the wake of the rise of new wave of individualization 'the individual is increasingly viewed today as an active agent in the risk-monitoring of collectively produced dangers; risk-information, risk-detection and risk-management is more and more constructed and designed as a matter of private responsibility and personal security. By and large, human agents confront socially produced risks individually. Risk is de-socialized; risk-exposure and risk-avoidance is a matter of individual responsibility and navigation. This is, of course, partly what Beck means by the individualization of risk' [107]. It has been contended, on the basis of a study of world risk society in relation to the terrorism-crime nexus, that private security business contributes 'tothe rise of a culture of fear in which the demand for security can never be satisfied and guarantees continuous profit' [108]. While some researchers find that in CC security risk, for instance, of data storage is still 'critical' impeding CC's adoption[109], others point to the prevailing absence of 'structured method' for risk assessment (viz. risk identification, assessment and mitigation) for consumers in the domain of CC [110].

Fourth, in the concerned literatureand empirical research on CC, there exists in fact no consensus, let alone unanimity, on the number or type of threats, vulnerabilities or risks in view of the complexity, context or type of cloud adopted. Indeed, experts do differ on the matter. The case is similar with the risks in the risk society. What is important is that Smith, while reviewing Beck's view, states that 'the risk experts who provide the veneer of scientific and institutional credibility that makes such ventures seem manageable thus became part of the problem not the solution. Since they base their calculations and recommendations only on demonstrable chains of causal inferences that are, if Beck is correct, inherently unavailable in advance, they inevitably contribute to a process of 'risk denial" . Eventually the argument advances that the risk is either minimal, managed or contained [93]. Risks exist in scientific knowledge rather than in actual experience of the individual. However, the point is that experts contradict each other over indeterminate nature of risks or hazards 'resulting in debates over standpoints, calculation procedures and results. This also tends to paralyse action' [111]. Beck himself is rather causticabout risk determination or calculations by techno-scientific community [112]. 'Their safety monopoly drives them into a dogmatic mania for perfection, and precisely as 'perfection' comes under excessive strain, opportunities are multiplied for public demonstrations of the insecurity of technical certainties and security. This takes place in the interplay of expert opinions, as exact as they are divergent; in the quick change of 'advances in knowledge', now in one direction, now in another; in the open plurality of risk studies; and in the style of wrestling that will of necessity decide the outcome of the struggle'[112]. Likewise, the principle of compensating in case failure of safety or security has also changed now. 'The logic of compensation breaks down and is replaced by the principle of precaution through prevention. Not only is prevention taking precedence over compensation, we are also trying to anticipate and prevent risks whose existence has not been proven' [113].

Finally, one of the features of CC is that its services are 'available anytime and anywhere' [109]. That is, the CC is both global and globalizing. The same is true of the risks in risk society. They possess 'an inherent tendency towards globalization' where industrial production takes place independent of location and is thus not limited to the nation-state or any national borders (e.g., acid rain, climate change etc.)[101] [104][109]. Globalization is multifaceted including dimensions such as '*communications technology, ecology, economics, work organization, culture* and *civil society*' [114].The role of information technology is crucial in creating a global risk society. 'The global market risk is a new form of 'organized irresponsibility' because it is an institutional form so impersonal as to have no responsibilities, even to itself. Enabled by the information revolution, the global market risk allows the near-instant flow of funds to determine who, if any one, will prosper, and who will suffer' [105].

While analyzing the consequences of the Fourth Industrial Revolution Schwab draws attention to the emergent risky scenario on the whole in these words: 'The challenge of externalities and unintended consequences is particularlyacute given the power of Fourth Industrial Revolution technologies, and the uncertainty as to their long-term impacts in complex social and environmental systems. At the most alarming level, risks range fromattempts at geoengineering that could lead to sudden and irreversibledamage to the biosphere, or the development of an artificial general intelligence whose goal-seeking behavior clashes with the diverse messiness of human life. By making swathes of existing cryptographic approaches obsolete, under some scenarios quantum computing could create significantrisks to privacy and security for anyone able to access new computing approaches. The widespread use of private, autonomous vehicles could increase road congestion in already crowded cities. And the rise of virtual reality may further exacerbate the challenge of online harassment, making it even more psychologically damaging' [4].

Against the background of preceding analysis it may indeed appear that risks in CC and risks in the risk society portray only the darker sides of a technology and social institutions of industrial risk society. However, there are more reasons to be optimistic than is really warranted by any appraisal of the risks of both for overdetermining reasons in favour of progressive development of innovations in the domain of science and technology, and social life. It is of course the rise of scientific and computing innovations will inevitably affect the life and experience of the individuals and social institutions in more ways than one in this late modern society. The world which has become riskier than before does not mean that risks are always inherently negative for often the business entrepreneurs are often rewarded in risky ventures or even in scientific and technological investigations. Risks open up the future giving a wide arena of novel choices for individuals and organizations that did not exist before. Giddens, a contemporary of Beck, reminds one of these positive aspects. 'Manufactured risk is expanding in most dimensions of human life. It is associated with a side of science and technology which the early theorists of industrial society by and large did not foresee. Science and technology create as many uncertainties as they dispel – and these uncertainties cannot be 'solved' inany simple way by yet further scientific advance. Manufactured uncertainty intrudes directly into personal and social life – it isn't confined to more collective settings of risk. In a world where one can no longer simply rely on tradition to establish what to do in a given range of contexts, people have to take a more active and risk-infused orientation to their relationships and involvements'[115]. Even Beck himself was not a pessimist in his search for solutions of the newly arisen risks of late modern era since the 1970s. He cautiously reminds: 'We are living in an age technological fatalism, an 'industrial middle ages', that must be overcome by more democracy—the production of accountability, redistribution of the burdens of proof, division of powers between the producers and the evaluators of hazards, public disputes on technological alternatives. This in turn requires different organizational forms for science and business, science and the public sphere, science and politics, technology and law, and so forth'[105].

In the current CC domain, remarkable developments and innovations continue to grow. The **CC,** along with big data and new algorithms are contributing to the development of 'Platform Economy' as a part of third globalization, 'reconfiguring globalization' itself' [116]. It is also at the base of post-cloud computing paradigms such as Fog Computing, Mobile Edge Computing, and Dew Computing. As Zhou et al. summarize its impact by saying that 'newly emerging post-cloud computing paradigms do not completely differ from cloud computing, but rather area natural extension of cloud computing from centralized to small-scale centralization and distribution, which can be regarded as a historical regression to the PC distributed computing paradigm [117]. Within the healthcare industry CC is making significant inroads.'Notable uses of cloud services have included vendor solutions aimed at storing large amounts of data for purposes of clinical trial research and business analytics, disaster recovery of mission critical systems, and significantly reducing the overall space within a hospital which is occupied by a physical data center'[118]. The CC is one of the vital enabling technology for Internet of Things (IoT) [119] defined as 'the idea of putting intelligence (usually through small computing devices, known as embedded systems) intophysical objects, so that relevant data can be collected from the objects nd sent to other devices for processing and decision-making' [120]. In view of challenges emanating from globalization, increasing ICTs, and energy consumption, CC has also become an integral part of cloud manufacturing (CM). 'By using CM it is possible to take a product through its entire lifecycle from planning all the way to disposal, while being controlled through cloud services' [121]. Leaving aside other CC applications in other areas social life (viz. education, publishing, IT call centres, etc), the compelling conclusion is that risks are a sort of 'social development' while global risks are a reality which need to be 'daringly tamed', for at the end of the day risks only 'drivers of social change' [122]. And in the present networked society, 'a matrix of random connections and disconnections with an infinite number of possible permutations' [123], one has only to dare to confront the issues head on. To conclude, therefore, in the words of Giddens: 'there can be no question of merely taking a negative attitude towards risk. Risks always need to be disciplined, but active risk-taking is a core element of a dynamic economy and an innovative society. Living in a global age means coping with a diversity of new situations of risk. We may need quite often to be bold rather than cautious in supporting scientific innovations or other forms of change. After all, one root word of risk' in the original Portuguese means to 'dare' [124].

ACKNOWLEDGEMENT: The author deeply and sincerely acknowledges the important assistance received from Retired Professor Bipul Kumar Bhadra, PhD (McMaster), of Jadavpur University, Kolkata.

References

[1] NIST (National Institute of Standards and Technology). October 25, 2011**.** Special Publication 800-145. Final Version of NIST Cloud Computing Definition Published. *https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published*, p.2-11. [Retrieved on 19 December 2019].

[2] Rifkin, Jeremy. 2011. *The Third Industrial Revolution*. New York: PalgraveMacmillan.

[3] Schwab, Klus. 2016. *The Fourth Industrial Revolution*. Geneva: World EconomicForum, p. 7, 11.

[4] Schwab, Klus. 2018. Shaping the Future of the Fourth Industrial Revolution. New York: Currency.

[5] Kumar, R. and R. Goyal. 2019, 'On Cloud Security Requirements, Threats, Vulnerabilities and Countermeasures: A Survey', *Computer Science Review*, 33: pp. v-vi.

[6] Aissam, M. et al. 2018. "Cloud Robotic: Opening a New Road to the Industry 4.0", in Nabil Debel
et al. (eds.): *New Development* and *Advances in Robot Control*, Singapore: Springer p. 2.

[7] Kavis, M. J. 2014. *Architecting The Cloud: Design Decisions for Cloud Computing Models (SaaS, PaaS, and IaaS).*,Wiley, p. 34.

[8]Mohamed, Arif. 09 April 2018. 'A history of cloud computing', *Computer Weekly. Com.* Retrieved from *http://www.computerweekly.com/feature/A-history-of-cloud-computing*.

[9] Sharma, M. et al. 2017. 'Cloud Computing Risks and Recommendations for Security', *International Journal of Latest Research in Science and Technology*, 6(1), p. 52.

[10] R. Buyya, et al. 2013.*Mastering Cloud Computing Foundations andApplications Programming*, Amsterdam: Elsevier, p. 9.

[11]Baranwal G. et al. 2018. *Auction Based Resource Provisioning in Cloud Computing*, Springer: Singapore, p. 2.

[12]Pearson, S. 2013. 'Privacy, Security and Trust in Cloud Computing', in (eds.) S. Pearson and George Yee, (Privacy and Security in Cloud Computing (3-42). London: Springer

[13] Rebah, et al. (2018). in (eds.), T.F. Bissyande et al., *e-Infrastructure and e-Services for Developing Countries*, Springer: Switzerland, p. 7.

[14] DevTeam.Space Product Development Blog. 2020. 'Top 10 Cloud Computing Services Providers' , Retrieved from https://www.devteam.space/blog/top-10-cloud-computing-services-providers/ on February 04, 2020**.**

[15] Murugesan, S., and I. Bojanova. 2016. 'Cloud Computing: An Overview', in (eds.), S. Murugesan, and I. Bojanova, 'Encyclopedia of Cloud Computing', Wiley: Chichester. UK, p. 6, 10

[16]Belbergui, C. et al. 2019. 'Cloud Computing: Overview and Risk Identification Based on Classification by Type', in (eds.), M. Zbakh et al., *Cloud Computing and Big Data: Technologies, Applications and Security*, Springer: Switzerland, p. 22.

[17]Amara N. et. al. 2017. 'Cloud Computing Security Threats and Attacks with their Mitigation Techniques', 978-1-5386-2209-4/17 $31.00 © 2017 IEEE, DOI 10.1109/CyberC.2017.37, p. 245.

[18] Bhowmik, S. 2017. *Cloud Computing*, CambridgeUniversity Press: Cambridge, p. 272.

[19] Dahbur, K., et al. 2011. ACM 978-1-4503-0475-0/04/2011, p. 3.

[20] Jane, E.A., and E. Martellozzo. 2017. ‘ Introduction: victims of cybercrime on the small ‘i’ internet**’,** in (eds**.),** E. Martellozzo, E., and E.A. Jane,Cyber crime and Its Victims, Routledge: London, p.1.

[21] Brenner, S.W. 2010.*Cybercrime: Criminal Threats from Cyberspace*, Praeger: California, p. 10.23, 36.

[22] Hill, J.B., and N.E. Marion (2016), *Introduction To Cybercrime : Computer Crimes, Laws, and Policing in The 21st Century*, Praeger: California, p. 4,5-6.

[23] Clough, J. 2010. Principles of Cybercrime, Cambridge University Press: Cambridge, pp. 5-8.

[24] Willems, E. 2019. *Cyberdanger: Understanding and Guarding Against Cybercrime*, Springer: Switzerland, p. 187.

[25] Brar, H.S., and Kumar, G. 2016. ‘Cybercrimes: A proposed Taxonomy and Challenges’, *Journal of* Computer Networks and Communications, https://doi.org/10.1155/2018/1798659, p. 9.

[26] Wall, D.S., 2017. ‘Towards a Conceptualization of Cloud (Cyber) Crime’, in (ed.), T. Tryfonas, *Human Aspects of Information Security, Privacy and Trust*, Springer: Switzerland, pp.533-35.

[27] Mithunzi, S.N. et al.2019. ‘Cloud Computing Security Taxonomy: From Atomistic to Holistic View’, Future Generation Computer Systems’, *doi: https//doi.org/10.1016/j.future. 2019.11.013*, Sec. 4.2

[28] Kumar, R. and R. Goyal.2019. ‘On Cloud Security Requirements, Threats, Vulnerabilities and Countermeasures: A Survey’, *Computer Science Review*, 33, pp. 1-48.

[29]]Senyo, P.K., et al. 2018. ‘Cloud Computing Research: A Review of Research theme, Frameworks, Methods, and Future Research Directions, *International Journal of Information Management*, 38, pp. 128-39.

[30] De Donno, et al. 2019. Cyber-Storms Come from Cloud: Security of Cloud Computing in the IoT Era’, *Future Internet*, 11(127), pp. 1-30.

[31]Singh, S. et al. 2016. ‘A Survey of Cloud Computing Security: Issues, Threats, and Solutions’, ‘*Journal of Network and ComputerApplications*’, 75, pp. 200-22.

[32] Fernandes, D.A.B., et al. 2014. ‘Security Issues in Cloud Computing Environments’, *International Journal of Information Security*, 13, pp.114-70.

[33] Modi, C. et al. 2013. A Survey on Security Issues and Solutions at Different Layers of Cloud Computing’, *Journal of Supercomputer*, 63, pp. 561-92.

[34] Coppolino, L. et al. 2017. ‘Cloud security: Emerging threats and current solutions’, *Computers and Electrical Engineering*, 59, pp.1-17.

[35] Khalil, I.M. et al. 2014. ‘Cloud Computing Security:A Survey’, *Computers*, 3, pp. 1-35

[36] Latif, R., et al. 2014. ‘Cloud Computing Risk Assessment: A Systematic Literature Review’, in (eds.). J.J. (J.H) Park, *Future Information Technology*, Springer: Heidelberg, p. 285-95.

[37] Zissis, D. and D. Lekkas. 2012. ‘Addressing Cloud Computing Security’, *Future Generation Computer Systems’*, 28, pp. 583–592

[38] Asvija,B. et al. 2019. ‘Security in Hardware assisted Virtualization for Cloud Computing-State of the Art Issues and Challenges’, *Computer Networks*,151, pp. 68-92.

[39] Litchfield, A. and A. Shahzad. 2017. ‘A Systematic Review of Vulnerabilities in Hypervisors and Their Detection’, *Twenty-third Americas Conference on Information Systems, Boston, 2017, pp. 1-10.*

[40] Zafar, F. et al. 2017. ’A Survey of Cloud Computing Data Integrity Schemes: Design Challenges, Taxonomy and Future Trends’, Computer & Security, 65, pp.29-49.

[41] Cloud Security Alliance (CSA (2019), Top Threats to Cloud Computing: The Egregious 11, https://cloudsecurityalliance.org,. p 5, 4, 13, 25.[Accessed in 04 January, 2020].

[42] Deshpande, P.S., et al. 2019.*Security and Data Storage Aspect in Cloud Computing*, Springer Nature: Singapore, p. 7, 9-10

[43] Parikh, S., et al. 2019. ‘Security and Privacy Issues in Cloud, Fog and Edge Computing’, *Procedia Computer Science*, 160, p.736.

[44]Maniah et al. 2019. ‘Survey on Threats and Risks in the Cloud Computing Environment ‘, *Procedia Computer Science*, 161, pp.1330-31.

[45]Akshaya, M.S. et al. 2019. (Taxonomy of Security Attacks and Risk Assessment of Cloud Computing’, in (eds.), Peter, J.D. et al., *Advances in Big Data and Cloud Computing*, Springer: Singapore, pp. 48-50.

[46]Hashizume, K., et al. 2013. ‘An Analysis of Security Issues for Cloud Computing’, *Journal of Internet Services and Applications*’, 4-5,pp. 1-6.

[47] Deshpande, P. et al. 2018. ‘Security and service assurance issues in Cloud environment’, *International Journal of System Assurance Engineering and Management*, 9(1), pp. 195, 198.

[48] Latif, R. et al. 2014.‘Cloud Computing Risk Assessment: A Systematic Literature Review’, in (eds.), J. J. (Jong Hyuk) Park et al. (eds.), *Future Information Technology*, Springer: Heidelberg, p.293.

[49] Martins, A., and J. Eloff. 2002. ‘Information Security Culture’, in (eds.), E.A. Ghonaimy et al., *Security in the Information Society: Visions and Perspectives*, Klumer: Massachusetts, pp. 203-4.

[50] von Holms. B. 2000. ‘Information Security-The Third wave’,*Computers and Security’*, 19(2000), pp.615-6.

[51]Kraemer, S. and P. Carayon. 2005. ‘Computer and Information Security Culture’, *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting-2005*, pp. 1483-1487.

[52] K-L, Thomson et al. 2006. ‘Cultivating an Organizational Information Security Culture’, *Computer Fraud & Security*. 2006 (October), 7-11.

[53] von Solms, R. and J. van Niekerk. 2013. ‘From Information Society to Cyber Security’, *Computers & Security*, 38, pp. 97-102.

[54] Reid, R. and J. V. Niekerk. 2014. ‘From Information Security to Cyber Security Cultures’. *978-1-4799-3383-9/14/$31.00 ©2014 IEEE*, (November) 2004.

[55] Pichan, A., et al. 2015. ‘Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis, *Digital Investigation*, 12, pp. 52-4.

[56] Soomro, Z.A., et al. 2016. ‘Information Security Management Needs more Holistic Approach: A Literature Review’, *International Journal of Information Management*, 36, pp.215-25.

[57] Da Veiga and N. Martins. 2017. ‘Defining and Identifying Dominant Information Security Cultures and Subcultures’, *Computers & security*, 70, 72-94.

[58] Simmonds, M. 2018. ‘Instilling a Culture of Data Security throughout the Organization’, *Network Security*,(June) 2018, pp.9-12.

[59] Merhi, M.I. and P. Ahluwalia. 2019. ‘Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security’, *Computers in Human Behavior*, 92, pp. 37-46.

[60] Angraini. et al. 2019. ‘Information Security Policy Compliance: Systematic Literature Review’, *Procedia Computer Science*, 161, pp. 1216-24.

[61] Paananen, H. et al. 2020. ‘State of Art in Information Security policy Development’, *Computer & security*, 88, pp. 1-14.

[62] Renaud , K., et al. 2018. ‘Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious?’,*Computer Security*, 78, p.207.

[63] Devi, S. and M. A. Rather. 2019. in (eds.), ‘Cyberspace and Cyber security in the Digital Age: An Evolving Concern in Contemporary Discourse’,, in (eds.),Gupta, B.B., et al., *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*, CRC Press: London, p. 96.

[64] Schlienger, T. and S. Teufel. 2002. ‘Information Security Culture’, in (eds.), E.A. Ghonaimy et al., *Security in the Information Society:Visions and Perspectives*, Klumer: Massachusetts, pp. 196.

[65] Huang, K. and K. Pearlson. 2019. ‘For What Technology Can’t Fix: Building a Model of Organizational Cybersecurity Culture’, *Proceedings of the 52nd hawaii International Conference on system science 2019*, URL://hdl.handle.net/10125/60074, p. 6398.

[66] Maroc, S., and J. Zhang . 2019. 'Comparative Analysis of Cloud Security Classifications , Taxonomies, and Ontologies', https://dot.org/10-1145/3349341.3349487,
pp. 666-72.

[67] ENISA (European Union Agency For Network and Information Security). 2018. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, ENISA: Greece, p.5.

[68] Belbergui, C. et al. 2019. 'Cloud Computing: Overview and Risk Identification Based on Classification by Type', in (eds.), M. Zbakh et al., *Cloud Computing and Big Data: Technologies, Applications and Security*, Springer: Switzerland, p. 24.

[69] ENISA, 2017. '*Cyber Security Culture in Organizations*', ENISA: Greece, p.7.

[70]AlHogai, A., and Mirza, A. 2014. 'Information Security Culture: A Definition and A
Literature Review', *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, DOI: 10.1109/WCCAIS.2014.6916579

[71] Mell, P. 2012. 'What's Special about Cloud Security?',*IT Pro*, (July/August 2012), p. 7.

[72] Amron et al. (2017), 'A Review of Cloud Computing Acceptance Factors, *Procedia Computer Science*, 124, p. 644.

[73]Singh, A., and K. Chatterjee. 2017. 'Cloud security issues and challenges: A survey' *Journal of Network and Computer Applications*, 79, p. 100-01.

[74] Quedraogo, M. et al. 2015. 'Security Transparency: The Next Frontier for Security Research in the Cloud', *Journal of Cloud Computing*, 4(12), p. 3.

[75] Caulkins, B. et al. 2019. Cybersecurity Skills to Address Today's Threats', in (eds.), T.Z. Ahram and D. Nicholson, *Advances in Human Factors in Cybersecurity*, Springer: Switzerland, p. 188.

[76] Wiley, A. et al.2020. 'More than the Individual: Examining the Relationship between Culture and Information security Awareness', *Computer & Society*, 88 (101640), pp. 1, 3.

[77] Sultanand van de Bunt-Kokhuis2012. 'Organizational Culture and Cloud Computing: Coping with a Disruptive Innovation', '*Technology Analysis& Strategic Management'*, 24(2), p. 173.

[78] Govender, S.G., et al. 2018. 'Enhancing Information Security Culture to Reduce Information Security Cost', in (eds.) Castiglione, A., et al., *Cyberspace Safety and Security*, Springer: Switzerland., p.285

[79] Yu, Z. et al. 2017. 'A Descriptive Literature Review About Cloud Computing Security Research in the IS Discipline', *2017 International Conference on Computer Science and Application Engineering (CSAE 2017)*, p. 423.

[80] Singh, S. et al. 2016. 'A Survey of Cloud Computing Security: Issues, Threats, and Solutions', '*Journal of Network and ComputerApplications*', 75, p. 204

[81] Menzi, H. et al. 2018. 'The Uncertain Cloud: State of the Art and Research Challenges', *International Journal of Approximate Reasoning*, 103, pp. 139, 142.

[82]Almubaddel, M. and A. M. Elmogy. 2016. 'Cloud Computing Antecedents, Challenges, and Directions',*DOI: http://dx.doi.org/10.1145/2896387. 2896401*.

[83] Gartner, 'Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019', April 2, 2019.https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g.[Retrievedon February 7, 2020].

[84] Karwasra, N. and M. Sharma 2012. 'Cloud Computing: Security Risks and Its
Future', IJCSCE *Special issue on "Emerging Trends in Engineering" ICETIE 2012*,pp. 8-9.

[85]Gupta, D. 2018. 'Cloud Computing India: adoption, benefits, and challenges, *https://yourstory.com/mystory/dbd4732823-cloud-computing-in-ind*. Retrieved on February 2, 2020.
[86]Nasscom. 2019. 'Cloud: Next Wave of Growth in India 2019', Noida: Nasscom, p. 5.

[87] Chang, J. 2020. '101 impressive Cybersecurity Statistics: 2019 &2020 Data & Market Analysis ' ,https://financesonline.com/cybersecurity-statistics/.[Retrieved on 10 January 2020].

[88] Sobers, R. 2019.*110 Must-Know Cybersecurity Statistics for 2020*, https://www.varonis.com/blog/cybersecurity-statistics/.[Retrieved on 19 January 2020].

[89]Samarati, P. andS. D C. D. diVimercati. (2016), 'Cloud Security: Issues and Concerns'. in (eds.),S. Murugesan and I. Bojanova, *Encyclopaedia of Cloud Computing*, Wiley: UK, p. 207.

[90] Cybersecurity Insiders. 2018. *2018 Cloud Security Report*PDF, pp. 6, 8, 10.

[91] Cloud Security Alliance(CSA).2018. State of Security 2018, https://cloudsecurityalliance.org/geab, pp. 9-10.

[92] Mythen, G.2004. Ulrich Beck: A Critical Introduction to the Risk Society, Pluto Press: London, p. 5.

[93] Smith, M.2005. 'Risk Society and Ethical Responsibility', *Sociology*, 39(3), p. 543

[94]*Sørensen, M.P. and A. Christiansen* ,Ulrich Beck:An introduction to the theory of second modernity and the risk society, Routledge:London, 2013, p. 123, 12, 16-7., 21, 29-33.

[95] Summerton J. and B. Berner.2003. 'Constructing risk and safety in technological practice An introduction', in (eds.) J. Summerton and B. Berner, *Constructing Risk and Safety in Technological Practice*, Routledge: London, pp. 4-23.

[96]Bialostok S.and Robert Whitman. 2012. 'Education and the Risk Society: An Introduction', in (eds.), Bialostok S. et al., Education and the Risk Society, Sense Publishers: Rotterdam, pp. 8-14.

[97]Zinn, J.O. 'Recent Developments in Sociology of Risk and Uncertainty', *Historical Social Research*, 31(2), pp. 276-81.

[98] Porter, R 2002.*Review* of 'The Risk Society and Beyond: Critical Issues in Social Theory', *Contemporary Political Theory*, 1, p.392.

[99]Beck, U. 2014. 'Ulrich Beck's Scientific Leadership Profile', in *U. Beck, Pioneer in Cosmopolitan Sociology and Risk Society*. Springer: Munich, p. 3.

[100] Beck,, U. 1996. 'Risk Society And The Provident State', in(eds.) Lash et al., *Risk, Environment & Modernity: Towards a New Ecology*. Sage: London, p. 28.

[101] Beck,, U. 1990. 'On the Way Toward an Industrial Risk Society of Risk?',*International Journal of Political Economy*', 20(1), pp. 53, 61-2.

[102] Beck,, U. 1990. *World at Risk*, Polity: Cambridge, pp. 8, 13

[103]Acterberg, W.2001. 'Democracy, Justice and Risk Society: The Meaning and Shape of Ecological Democracy',in (eds.), John Barry and M. Wissenburg,*Sustaining Liberal Democracy*. Hampshire: Palgrave, pp. 102-03.

[104] Beck, U.1992. *Risk Society: Towards a New Modernity*. Sage: London, pp.20, 46, 59-60, 175.

[105] Beck, U. 1999. *World Risk Society*. Polity: Cambridge, pp 2. 6, 70.

[106] Srinivasan, S. 2014. *Cloud Computing Basics*, Springer: New York, p. 101.

[107] Elliott, A. 2002. 'Beck's Sociology of Risk : A Critical Assessment', *Sociology*, 36(2), pp. 305-6.

[108]Krahmann, B. 2011.'Beck and Beyond: Selling Security in the world Risk Society', *Review of International Studies*, 37, p.371.

[109]Berrezzouq, M. et al. 2019. 'Issues and Threats of Cloud Data Storage', in (eds.), M. Zbakh et al,
Cloud Computing and Big Data: Technologies, Applications and Security, Springer: Switzerland, pp.60, 70.

[110] Drissi S. et al. 2013. 'Survey: Risk Assessment for Cloud Computing',
(IJACSA) International Journal of Advanced Computer Science and Applications, 4(12), p.147.

[111] Lupton, D. 1999. *Risk*. Routledge:London, p. 66.

[112] Beck, U. 1995. *Ecological Politics in an Age of Risk*, Polity: Cambridge, pp. 9, 177.

[113] Beck, U. 'Living in the world risksociety', Economy and Society, 35(3), p. 334.

[114] Beck, U.2000. What is Globalization?, Polity: Cambridge, p.19.

[115] Giddens, A. 1999. 'Risk and Responsibility', *The Modern Law Review*, 62(1), p. 4.

[116] Kenney, M., and John Zysman (2016),, 'The Rise of the Platform Economy', Issues in science and technology, Spring , p.1.

[117]Zhou, Y., et al. (2017), ‘Post-Cloud Computing Paradigms: A Survey and Comparison’, *Tsinghua Science and Technology*, 22(6), p .719.

[118] Faix, R. and E. Gerard. 2018. ‘Healthcare Industry’ in (eds.), D.M. Groom and S. Jones, *Enterprise cloud computing for non-engineers*, CRC Press: Florida, p. 64.

[119] Sharma, S., et al. 2019. ‘Cloud and IoT Based Emerging Services Systems’, Cluster Computing, 22, pp. 71-91.

[120]Chandler, N. 2018. ‘The Internet of Things’, in (eds.), D.M. Groom and S. Jones, *Enterprise cloud computing for non-engineers*, CRC Press: Florida, p. 106.

[121]Buckholtz, B. et al. 2015.‘Cloud Manufacturing: Current Trends and Future Implementations’, *Journal of Manufacturing Science and Engineering*, 137(August), p. 040902-1.

[122] Kovacevik, B. and I.Kovacevik, 2017. *Sociology of Global Risk Society*, Banja Luka: European defendologycenter for scientific, political, economic, social, safety, sociological and criminological research, p. 52.

[123] Bas, E. ‘The Liquid Self: Exploring the Ubiquitous Nature of the Future Internet and Its Pervasive Consequences on Social Life’, in (eds.), J. Winter, and R. Ono, *The Future of Internet*:*Alternative Visions*, Springer:Heidelberg, pp. 194-5.

[124] Giddens, A. 2002. *Runaway World: How Globalisation is Reshaping our Lives*, Profile Books: London.