SECURING CLOUDY CYBERSPACE: AN OVERVIEW OF CRIMES, THREATS AND RISKS

SOMPURNA BHADRA

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

Abstract:- *The present paper gives a general overview of issues confronting cloud computing (CC) which has now become very popular. It is because it allows a novel way of providing computing resources and services to users on internet in view of rapid development of network technology. However, its locale in the cyberspace has been subjected to numerous onslaughts of cybercrime and cloud crimes. This requires inclusion certainly of cyber and information security cultural elements in the framework of cloud threat management in the content of security or control measures. Further, the development of CC in this era of late modernity has added a new dimension in strengthening late modern society into a risk society. All these aspects have addressed in this paper from an interdisciplinary behavioural cyber security perspective. The paper ends optimistically by urging challenging researches on how to prevent and remove uncertainties and uncontrollabilities prevailing in the cybersphere and cloud computing.*

Key Words: Cloud Computing, Cyberspace, Security Measures, Cyber and Cloud Crimes, Cyber and Information Cultures, Cloud Threats, Risk Society

.

I. INTRODUCTION: WHAT IS CC?

Rapid expansion of internet usage world-wide has made it easier to manage the increasing volume and availability of data through the use of CC. It enables any one to access data from any place in the world via the internet. NIST (The National Institute of Standards and Technology).defines cloud computing as 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'. NIST also enumerates five characteristics CC. 1. On-Demand Self-Service. 2. Broad Network Access.3. Resource Pooling. 4. Rapid Elasticity and 5. *Measured Service* [135]. The following figure 1, taken from Dataflair Team, exhibits as many as 10 features as shown below [136].

Figure 1. Features of Cloud Computing

NIST lists three CC service models. The first one is Software as a Service (SaaS). It is provided by consumers to use the provider's applications running on a cloud infrastructure which is a collection hardware and software and contain 'both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer'. The second one is *Platform as a Service* (PaaS)which gives the consumer the capability 'to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider'. Thirdly, *in Infrastructure as a Service* (IaaS) servicing the consumer is enabled 'to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications' [135].The following Figure 2 depicts capability and controllability of the user in the three servicing models [137].Figure 3 show three deployment models.

Service model	Capability offered to the user	Controllability by users
Software as a service (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 a service (PaaS)	Deployment of applications on the cloud infrastructure; may use supported programming languages, 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 as a 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

Cloud services are related to customer requirements depending generally on the size of the organization concerned, and hence cloud deployment models are chosen accordingly. Small and medium sized businesses usually use Public Cloud in which infrastructure and computing resources are offered over a public network. Large organizations use Private Cloud for computing services in which management and control rest with the organizations itself or a cloud provider. Naturally, it offers highest data security and more control over the infrastructure. Hybrid cloud is mixture of two or more types of deployment models (public, private or community) in which concerned organizations combine for sharing computing resources or data without affecting each other. Community cloud is a sort of public cloud formed for, and limited to, a group of consumers having a common interest and hence will share resources having shared concerns [121.]

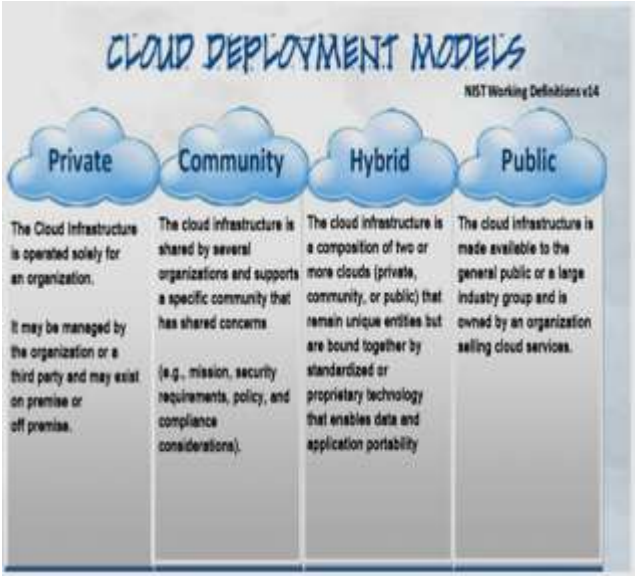

Figure 3 shows the four essential deployment models of CC [138]

The strategy of this paper is as follows: In section II security measures for CC are discussed, while in section III the importance of security issues and dimensions related to cyberspace are detailed, Section IV explores lessons from Information Security Culture and Cyber Security Culture as integral components of CC security measure. The threat issues of cyber crimes and cloud crimes are taken up in the next section V. Finally, the last section VI contains conclusions emphasizing uncertainty and risks facets of CC in the transitional era of liquid modernity in the risk society.

II. TOWARDS THE SECURITY MEASURES: PREMINARY REMARKS

Giddens, a world renowned sociologist, while evaluation the transformations of the human society in the current modern society, poignantly remarks that character of the so-called modernity. post-traditional social order is marked by two dominant themes: *'security versus danger* and *trust versus risk'*. It is, as if, the process of dialectics is on. As he says, 'The development of modern social institutions and their worldwide spread have created vastly greater opportunities for human beings to enjoy a secure and rewarding existence than any type of pre-modern system. But modernity also has a sombre side, which has become very apparent in the present century'. The consequences of modernity are such that living in the modern world, as contrasted with that in the pre-modern one, is not simply 'happier and more secure' but is especially 'fraught and dangerous' [1]. This is equally, if not in a more straightforward manner, echoed by Bauman who affirms that we are living in an age of uncertainty called Liquid Times. We are passing from the

'solid' to the 'liquid' phase of modernity, meaning thereby 'into a condition in which social forms (structures that limit individual choices, institutions that guard repetitions of routines, patterns of acceptable behaviour) can no longer (and are not expected) to keep their shape for long, because they decompose and melt faster than the time it takes to cast them, and once they are cast to set for them to set' [2].He thus terms this transitional era of liquid times as the era of liquid modernity [3] in which risk becomes an integral component of modernity. Modernity tantamounts to what Giddens call 'risk culture'. It means that risk becomes entrenched in the way 'both lay actors and technical specialists organise the social world' [4]. To extend further the argument, risk culture is the culture of modernity or modern society. For Beck, the risk society is a kind of society that systematically produces, defines and distributes 'techno-scientifically produced risks'. Accordingly, (risk) problems and conflicts in such a society arise 'from the production, definition and distribution of techno-scientifically produced risks' [5].

While more will be said in this regard, it is necessary to point to another transition that is taking place on the wake of the rise of Information and Communications technologies (ICTs) since the 1970s onward. The ICTs inaugurated what is known as known as 'information or digital age' when internet, email, social websites and satellites came to pervade and revolutionize every sphere of life. It was heightened by the process of globalization whereby every part of world became interconnected [6].Moreover, globalization of technology also stands for accelerating facilitates transmission of knowledge and spur innovations, which can lead to economic development in the developing societies [7]. In the yearly years of the 2010s it is reported that an average person has five connected devices – PCs, laptops, cell phones, tablets, etc—each containing potential for information. Each day 294 billion e-mails and 5 billion phone messages were exchanged. Global mobile traffic reached 2.5 exabytes each month at the end of the year 2014 [8]. Brar and Kumar (2018) inform that the number of devices is growing by leaps and bound in terms of both volume and variety and is likely to reach 200 billion by 2020. Nearly 50% of the world total population has internet connection up to January 2017. In 2016 there were 6.4 billion connected devices but the figure is likely to go up to 20.8 billion by 2020. This rise in scale and volume created an exponential growth of data creating almost a gigantic cyberspace [9]. It has, in turn, has become habitat not only of much sought after utilities but also more especially what is known as cybercrimes or computer crimes.

The terms cyberspace was first used in 1984 by William Gibson in his novel *Neuromancer*. Today the term cyberspace, according to Zaharia, 'usually refers to the common space created by any combination of hardware and software that is at the base of the Internet and offers support for any facility offered to the user. The various faces of cyberspace are similar to the main directions of Internet application development, which are: networked media and search systems, cloud computing, Internet services, trustworthy computing, and the 'future Internet.' Cyberspace consists of hardware, operating systems, communication networks, and applications. There is a supplementary layer composed of the frameworks that allow the execution of applications' [10]. Cyberspace is often equated to homogenous virtual public or common space. But, says Bell, 'this is surely to cloak the multifarious usages of ICTs. More accurately, cyberspace should perhaps be regarded as a collection of different multimedia technologies and networks which, while they may be held together by the standard computing protocol (TCP/IP), do not necessarily imply that visitors to cyberspace can access all of its domains. Thus while some usages of the Internet , such as encrypted person-to-person email , invited IRC or video conferencing, and password protected FTP or World Wide Web sites may be relatively private, others such as email-based distribution lists, Usenet groups and WWW pages are more public in orientation' [11]. Instead of being a homogeneous space, cyberspace it is 'a myriad of rapidly expanding cyberspaces, each providing a different form of digital interaction and communication. In general, these spaces can be categorised into those existing within the technologies of the Internet, those within virtual reality, and conventional telecommunications such as the phone and the fax, although because there is a rapid convergence of technologies new hybrid spaces are emerging' [12]. In brief, cyberspace is not a geographical place but a borderless 'space' transformed by networks of information and communication' [13]. Cyberspace does indeed offer numerous advantages. It facilitates social interaction without physical presence, provides a forum for discussion and exchange of ideas, enables business transactions, gives a platform for political debates, furnishes opportunities for enjoying leisure or playing games, and so on [11]. It is giving rise to what is called 'network sociality' consisting of 'fleeting and transient, yet iterative social relations; ephemeral but intense encounters' [14].And this modern society is not only 'on the move' [15] but also a 'network society [16].

Nielsen lists seven key features of the cyberspace domain, these are as follows: First, cyberspace was built to support particular purposes such as ease of access, availability, interoperability, exapansionability, and innovation. Second, it is dynamic in the sense that its structure can change rapidly. Third, cyberspace is fast because events in cyberspace can happen speedily, almost instantaneously. Fourth, cyberspace is relatively without borders, relatively in view of conflict between laws and regulations of sovereign states. Fifth, cyberspace has very low barriers to entry or access. Sixth, cyberspace is growing rapidly in view of innovations and implementations of new supportive technologies. For instance, internet users increased from about 16 million in 1995 to almost 2.3 billion by the end

of 2011, which is equal to about 33 per cent of about 6.9 billion world population [17]. In 2018, there were nearly 4 billion internet users, nearly half of the world population of about 7.7 billion, up from 2billion in 2015. The prediction is that the figure will be 6 billion by 2022, which is 75 percent of the projected world population of 8 billion. Further, there will be more than 7.5 billion internet user by 2030, constituting 90 percent of the projected world population of 8.5 billion. The World Wide Websites, which was invented in 1989 and first ever website went live in 1991, now number at nearly 1.9 billion websites. It is predicted that total amount of data stored in the cloud will be 100X greater in 2021 than it now today. Further, in Big Data in IoT, 2 billion objects (smart devices communicating wirelessly) in 2006 will jump to projected 200 billion by 2020. The world's digital content is predicted to increase from 4 billion terabytes in 2016 to 96 zettabytes by 2020[18].Finally, following Nielsen again the seventh feature of cyberspace is that it can be viewed from diverse perspectives through a variety of frames which inevitably shape influencing what is appropriate behaviour and values in the society. The perspective on the beneficial dimensions has been discussed. But the relevant issue, the other perspective, relates to the dimensions of 'security challenges in cyberspace in risk management' of threats, vulnerabilities and resultant detrimental consequences--social, political, economic, etc. [17].

The point is to ensure the safer cyberspace and realizing the benefits, goals and efficacy of the technological breakthrough known as the Fourth Industrial Revolution, i.e. Industry 4.0 [19]. When cyberspace continued to grow with the increasing and ubiquitous usage of internet, the emergence of computer or cybercrime cannot be far behind, as indicated earlier. If the 1980s were a decade of computer-crime growth, the 1990s marked an explosion of computer crime witnessing more prevalent and devastating cyber attacks. In the early 21st century internet became a' hotbed' of cybercrimes and usage of cyberspace in every way became a reality [20]. It is stated that cybercrime is now the 'greatest threat' faced by any economy in the world and one of the 'biggest' problem with mankind. What is more, especially in cloud environment, cyber attacks amplify and spread in view of the character of its larger infrastructure and this feature in cloud known as velocity of attack (VOA) [21]. As Bernik put it precisely, 'cyber attacks are extremely fast and can affect thousand or even millions of electronic devices within moments anywhere in the world' [22] Looking at the statistics, the figures of cybercrimes are quite overwhelming. In 2017 more than 978 million adults in 20 countries were affected by cybercrime. In China352.70 and in India 186.44 million adults experienced cybercrime. The average victim lost US $142 in the same year [23]. It is predicted that cost of cybercrime in the world will increase from US$ 3 trillion in 2015 to US $6 trillion by 2021. The cost includes damage and destruction of data, stolen money, theft of personal and financial data, fraud, embezzlement, restoration and deletion of hacked data and systems, etc. Business fell victim to a ransomware attack every40 seconds and is like to experience this attack every 14 seconds by 2019 and every 11 seconds by 2021. In 2016 healthcare, manufacturing, financial services, government, and transformation were the most 5 cyber attacked industries [18]. From 2019 to 2022, the top 10 most targeted industries for cyber attack are healthcare, manufacturing, financial services, government, transportation, retail, oil and gas/energy and utilities, media and entertainment, legal, and education. In 2018, the most common cyber attacks against companies were phishing (37%), network intrusion (30%), inadvertent disclosure (12%), stolen/lost device or records (10%), and system misconfiguration (4%). In 2013 Yahoo experienced biggest data breach of all time affecting 2 billion accounts. Between 2014 and 2018, this figure is 500 million for Marriott. By 2020 DDoS attack will reach 14.5 million by 2022. Hacking tools and kits for all types of cybercrimes are available online for only US$ 1. Finally, the global cybercrime economy makes a profit about US$ 1.5 trillion annually [24]. 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 [25]. Needless to say, the growth of cybercrimes worldwide is quite exponential. It is not going away either. Rather, their numbers are very likely to be more sophisticated and wider in scope. The reason is that every technological advancement tends to increase cyber attack incidents. 'Innovations like IoT, mobile payments, and cloud computing, unfortunately, have given birth to new sophisticated cybercrime activities' [24].Add to this the common objectives [9] behind perpetration of cybercrimes. The first is entertainment when the cyber criminals test their ability to attack the cyberspace and often enjoy and feel proud in case of success. Secondly, hactivism is motivated by political, religious social ends. Thirdly, they prompted by motives of financial gain. Fourthly, there is the specific purpose of espionage. Fourthly, there is the drive for taking revenge by insiders, especially the expelled, irritated or humiliated employees.

III. IMPORTANCE OF SECURIY ISSUES AND DIMENSIONS IN THE CYBERSPHERE

It has already been stated cybercrime are intrinsically dialectical. It can be looked at from different perspective [17]. That is, As Hill and Marion state: 'While advances in technology have benefited society, they have also created new opportunities for cybercriminals who use these innovations to cause harm to others. As technology has developed, so have new crimes that rely on that technology' [26].Against the backdrop of emerging voluminous and stunning cyber attacks it is indeed necessary to point to the necessity of securing the cyberspace and associated technologies so that cybercrimes can be prevented and remedied, if not

totally eliminated. However, before it can be done it is necessary to define a few relevant concepts that are fundamental to understand especially threats in the various types of computing environment including cloud computing.

First of all it is necessary to define the concept of cybercrime, occurring in 'hallucinogenic parallel universe known as The Cybersphere' [27] that has taken on exploding magnitude and dimensions in as discussed above. 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. 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' [28]. Cybercrime generally refers as Hill and Marion '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 or other 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'. He also cites 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, posting confidential business information on the Internet, committing identity theft or fraud, , money laundering and counterfeiting, and committing denial-of-service, malware; fake emails or websites; identity theft; cyberbullying, stalking, or harassment; hacking, credit card theft; or phishing etc.[26]. 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 [29].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 [30].

What follows from the above discussion of globalized and escalating cybercrimes in today's information-centric society is the need for their prevention and ensuring cyber safety or security even when it is common place to say that 100 per cent security will never be possible simply because, competing with the new and newer innovations in the ICTs, new vectors are surfacing and old ones can be exploited by novel ways [31]. Generally speaking, security protects 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. 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 [32].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--I wave, from the early 1980s to mid-1990s 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 o security awareness[33].Since then the importance of the theme of cybersafety continues reign among the concerned as reflected in the literature especially in the light of information and cyber security cultural analyses [34] [35][36][37][38][39][40][41][42][43]. It has been rightly argued 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 [37] [44]. The advent of the Information Revolution, precipitated by the ICTs have brought to the fore privacy and security issues and, so naturally, 'more significantly the concept of cyber security' [45]. And the security concerns require thus urgent attention from a systemic and holistic point of view.

Security challenges in cyberspace present a variety of threats, vulnerabilities, and risks. Bhowmik defines the concepts 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 a threat 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) [46]. 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 is designed 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' [47]. Since cyber security landscaper has drastically changed in view of new applications such as wireless technology, mobile applications, cloud computing, internet of things etc. [48], the countermeasures also vary.

In a recent significant publication Maroc and Zang provides cloud security classification framework on the basis of existing literature to facilitate the development of 'a unified and holistic framework for cloud computing security'. Their classificatory scheme cloud security literature into six categories. The first is service (SaaS, PaaS and IaaS) models-based and it considers the components and issues, which are not mutually exclusive, of each model. Secondly, by far the most widely accepted the component–based category, divided into technical, operational, and business, focus on the classes of security issues themselves but not on the basis of cloud service models. Third, the stakeholders role-based category focus on actors in regard to issues (e.g. malicious insiders or cloud abuse) which are not necessarily mutually exclusive since both cloud parties are involved. Fourth, the cloud-specific security issues-based classification, divided into specific and generic features, emphasizes the distinction between traditional security issues and cloud-specific issues. Fifth, the security attributes-based taxonomy concentrates on security and privacy attributes like confidentiality, integrity, availability, and privacy. Finally, composition-based classification attempts to combine different classification schemes to classify cloud security issues. It is important to note also in this context that there is not really one 'size that fits all classifications of cloud security issues due to inconsistencies and incoherencies that exist in the names and ways of referring to security issues and control. Moreover, they admit that there is no 'clear-cut line' between traditional security issues and new issues emerging from the cloud computing paradigm. Lastly the authors also draw attention to classifications based on cloud ontology (i.e. formalization of security knowledge regarding vulnerabilities, threats, and controls) which are as follows: resources and services description ontology, interoperability, ontologies, services discovery and selection ontologies, and security ontologies [49].

Against over-all preceding background discourse, the cyberspace domain has witnessed the rise of emerged two schools – information security culture and cyber security culture – that suggest certain controls to safeguard the cyberspace for managing the computing systems and employments.

IV.LESSONS FROMINFORMATION SECURITYCULTURE AND CYBER SECURITY CULTURE

As already indicated above, 100% security is not possible [50] *vis a vis* onslaughts against attacks on the computer technology assets from hackers in the cyberspace. Huang and Pearlson, two cyber security specialist at MIT instructively goes on to say that 'Even the most advanced technological 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' [51].Technological security remains incomplete simple because technology is after all 'dumb and deterministic' whereas humans are 'creative problem solver' [49]. 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 focal point. 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' [52].Indeed, the human factor or the people are the key factor in the failure or success of any information security management in AN organization for it vulnerable to attacks (e.g. hackers, viruses, pharming, financial scam, identity theft, data loss, and so on) from both inside and outside of the organization. If human factors are left unaddressed, organizations will very likely lose their ability to protect confidentiality, integrity and availability of the

information, which the trained and information security-aware employees can greatly aid to protect.[53][54]. Simmonds goes on to point out that 'cyber security is only as robust as its weakest link', and the fact is that 'the weakest part of 21st century business is likely to be its staff' [55]. It explains why the importance of human factors are being reinforced in the emerging discipline of behavioural cybersecurity, defined as 'the use of psychological, social, cognitive, and emotional factors as data to better understand, protect and defend information and communication systems from any unauthorized doings, or to encourage legitimate users to take better precautions' [56]. All this lies at the background of the rise of the information security culture and cyber security culture systems that afford sustainable computing systems, cloud computing included.

The concept of cyber security implies that solutions can be found for threats and attacks on the cyberspace in an all-encompassing contexts protecting information and on information-based assets of the individual, society or nation. von Solms and van Niekerk offer a descriptive definition by strongly stating that in cyber security 'information and ICT are the underlying cause of the vulnerability. It is still possible for the assets dealt with in security to include information itself, or even information and communication infrastructure. However, the single most defining characteristic of cyber security is the fact that all assets that should be protected need to be protected because of the vulnerabilities that exist as a result of the use of the ICT that forms the basis of cyberspace It involves mainly the protection of information and ICTs'[36]. In contrast, for Whitman and Mattord, information security is 'the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information'. It is not limited only to CIA triangle of confidentiality, integrity and availability but also includes features like accuracy, authenticity, utility and possession in view of constantly changing computing landscape. Two concepts of information security and cyber security are often used interchangeably but it is argued that the boundaries of the latter are wider than that of the former. That is, cyber security can be considered extension of information society [36]. While information security is about protection of information as an asset from various threats and vulnerabilities, 'cyber security is the protection of cyberspace itself, as well as the protection of those that *function in cyberspace* and *any of their assets* that can be reached via cyberspace'[37].

The two security concepts, cyber security culture (CSC) and information security culture (ISC), flow from or are associated with previously discussed concepts of information security and cyber security. The common factor is sociological dimensions of culture or behavioural dimensions covering many social sciences social sciences including sociology. Sociology is conceptualized as 'the scientific study of human society and social interactions'. Material Culture such as computer or ICTs are a type of culture which is defined as ' all that human beings learn to do, to use, to produce, to know, and to believe as they grow to maturity and live out their lives in the social groups to which they belong'. Nonmaterial culture consists of 'the *totality of knowledge, beliefs, values, and rules for appropriate behaviour.* The nonmaterial culture is structured by such institutions as the family, religion, education, economy, and government'. Finally, a social interaction involves *two or more people taking one another into account.* It is the interplay between the actions of these individuals. In this respect, social interaction is a central concept to understanding the nature of social life'. [57] Simply speaking, social interaction, the basis of society, is process in which two or more people become engaged but which influences the behaviour of the interacting parties. Drawing attention to the idiosyncratic nature of the human element, Frangopoulos, for instance, attempts to explain social engineering (SE) threats, its identification and control for information technology (IT) systems by applying traditional sociological principles along with sociological approach to technology (i.e. Actor Network theory, or ANT) taking due account of the role played by the social structures and interactions in the computing environment [58].

CSC and ISC are social and human countermeasures that supplement and complement technical measures that control or remedy cyber threats, attacks, vulnerabilities or risks in the computing environment, and hence this underpins their importance. Quite a lot of research literature is available, as can be guessed in the light of discussion above, on both CSC and ISC [36][40][41][44][50][51][59][60][61][62]. Cyber security culture, as ENISA (2017) conceptualizes, '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'[63].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 attack'* and the cybersecurity, being more than a technical issue the 'ultimate goal for manager is to drive cybersecure behaviors' among all organizational employees. The following Figure4 illustrated their cultural frame work [51]. The counterpart of CSC is 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 behavior in a

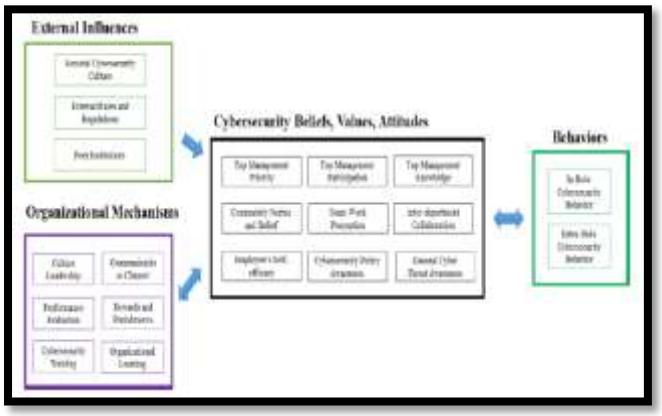

Figure 4Organizational Cybersecurity Culture Model

way that preserving the information security becomes a second nature'[64].Martins and Eloff contend that ISC consists of 'information security perceptions, attitudes and assumptions' that are endorsed and encouraged for acceptance in the ISC to protect information assets [65]. De Vega and Martins advocate for a stronger concept of ISC relating to protection of privacy as of ethical concern and hence advance the concept of information protection culture. They define it as 'a culture in which the protection of information and upholding of privacy are part of the way things are done in an organisation. It is a culture in which employees illustrate attitudes, assumptions, beliefs, values and knowledge that contribute to the protection and privacy of information when processing it at any point in time in the information life cycle, resulting in ethical and compliant behaviour' [61]

Recent researchers have endeavoured to reveal numerous dimensions to clarify the meaning and content of the CSC and ISC for defending against cyber security threats, vulnerabilities, attacks and risks basically caused by human and social factors.. For instance, Nasir and others in their review of the literature cite as 48 group of authors who, mostly in collaboration, have illustrated numerous and diverse and dimension of the ISC or factors changing ISC according to their own perspectives [66][40].Accordingly, many of them have also provided different models or frameworks for CSC and ISC to facilitate their utilization in the search for cyber countermeasures [41][50] [51][62][67][68]. At the same time, it may be noted that there is a dearth of available clear-cut information security policy literature. Angrani et al. point out that there remains a lack of research concerning 'the evaluation of information security policy compliance using specific metric and need to enhance the model of information security policy compliance with organizational theories' [69]. Paananen and other poignantly remark that there is still a need to clarify what information security policy means and how it can be formulated [70]. Finally, echoing the difference earlier noted between cybersecurity and information security, it is only a natural corollary to differentiate between the CSC ISC as Reid and van Niekerk do by CSC would have in the broader context of cyber space whereas ISC will be more relevant in the protected organizational environment [37]. The United Nations has encouraged the creations of a global culture of cybersecurity because 'technology alone cannot ensure cybersecurity' [71].

V. CYBER CRIMES AND CLOUD CRIMES

V.I.DUAL GENESES IN THE CYBERSPACE

Before examining the general view 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 1 by Brar and Kumar [9] 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 1 classification of cyber attacks on the basis of cyber crimes

In wake of the rise of networked and digital technology Wall suggests that cybercrimes scribes '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)'. He then suggests a cybercrime matrix [72] wherein developing cloud crimes are a subset of cybercrimes in Table 2.

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	DDoS Attacks, Mass hacks	Phishing, Ransomware	SNM, Hate speech

Table 2. A Cybercrime Matrix
(Mediation by technology v modus operandi)

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 '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' Cloud cybercrimes such as botnet crime-as- a- service, etc,, for example, are then facilitated by cloud technologies possessing massive computing power which in turn, with a multiplier effect, give rise to more complex cloud crimes. Visualizing a future scenario, Wall states: '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'[72]. The fluidity and uncertainty, implicit in the concept of liquid modernity of our times is manifest in cloud and cloud cybercrimes. However Stark and Tierney asserts that 'in computational terms, "liquid modernity" is already one phase transition behind the technological times' marked by term cloud computing [73].

While analysing the background of the rise of ISC and CSC components and the importance of their embodiment in the countermeasures to mitigate or eliminate risks in them, the pre-eminent role of the human, social, cultural or behavioural factors in the organizations was emphasised [41][51-56] [58] [63-64]. Even in the cloud security classification framework which called for facilitate the development of 'a unified and holistic framework for cloud computing security' Maroc and Zhang [49] draws attention to non-technical factors such as governance, compliance, and trust, malicious insiders, cloud providers, and cloud users, which falls short of what is required to protect invasions from the cyberspace. What is needed is to include a separate and distinct category of socio-cultural set of countermeasure in the overall taxonomy of cloud security countermeasure or controls. However, they rightly point out the predominance technical countermeasures and solutions in the extant literature on cloud computing. This is quite evident in the relevant literature dealing with, threats, vulnerabilities, attacks, and risks.

This is in spite of the confusions in the language used (viz., security concerns, security measures, security challenges, security issues, etc.) [74] [75] [76][77][78][79][80][81][82][83][84][85]. It should also be noted here that it is not true that no one refers to the human, or behavioural security measure to protect the cloud environment. Mell rightly argues that present security issues new use of 'the existing general purpose security controls'[86].For Example, Amron and others talk of 'human readiness' and management's support and ability [87], Mithunzi and others include 'human factor' as part trustissue in their general view of cloud computing[88], Singh and Chatterjee take in 'human aspect' as part of trust management [79],Quedraogo and others refer to employees' accidental or malicious tampering or leakage of data[89], 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 [90]. Caulkins 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[91]. 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'[92]. Sultan and Bunt-Kokhuis argues for 'a cultural overhaul of the way' the IT vendors used to do their business [93], 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'[62].

All this boils down to the fact that in preventing cloud risks the important requirement is to approach security problems can handled better in the cloud environment from an interdisciplinary perspective based on 'several disciplines , namely information systems, computer science, computer engineering, finance, accounting, and so on' [94]. Yu et al. strengthens the argument further: 'Cloud computing security research resides in an interdisciplinary area that includes technological, behavioural, managerial and social dimensions' [95]. Singh et al. include, in their classification of cloud computing security issues,, both ' human factors and forensics value' [96].Belbergui et al. [97] explicitly mentions human factors in threat sources in the following Figure 5.

V.II. SURVEYING THE CLOUD: SECURITY THREATS AND THEIR REMDIATIONS

Having outlined the role behavioural countermeasures to prevent pr-actively cloud computing risk which is indeed numerous, a brief survey of the threats in the cloud environment can now be presented. The relevant contemporary literature is quite rich in this respect. As evident in the contributions of Mithunzi et al. [88}, Kumar and Goyal [98] Senyo et al, [94], De Donno et al.

[99], Singh et al.[96], Fernandes et al.[82], Modi et al. [100],Coppolino et al. [78], Khalil et al. [83], Latif et al. [74], Zissis and Lekkas [84], Asvija et al.[101], Litchfield and Shahzad [102], Zafar F. et al. (103]. Recently, Mithunzi et al, (2019) have proposed a holistic view to facilitate 'comprehensive security analysis and the development of robust cloud security countermeasure'. In this regard, they discussed and summarized 11 perspectives to cloud security challenges: 1. Perspective of architectural complexities; 2. End-user perspective; 3. Outsourcing perspective; 4. Architectural, technological, process and regulatory perspective; 5. Traditional Computing

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 5Human threat sources in a cloud computing

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 hijackin	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 3 CSA top threats to cloud computing

and Cloud specific perspective; 6.Unique to cloud and pre-cloud perspective; 7. Cloud Layer perspective; 8. Co-residency perspective; 9. Outsourcing components of an organization perspective; 10. Data life cycle perspective; and 11. A general Perspective. They also proposed their own taxonomy of cloud security challenges [88].Kumar and Goyal (2019) exhaustively surveyed cloud security requirements including cloud vulnerabilities, threats and linkages between them including their pro- and reactive countermeasures [98]. The Cloud Security Alliance (CSA) lists of cloud threats (Table 3) which give the concerned an awareness of the prevailing the threats and changes in their rankings in the cloud environment [98] [104] in their 2019 Final Report 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' [104]. 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' [105]. Figure 6 exhibits it.

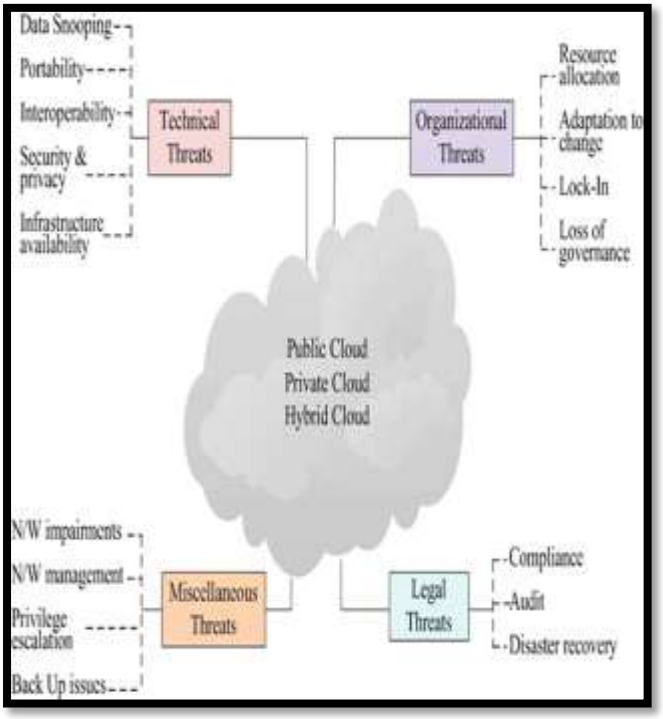

Figure 6 Threat classification of Cloud: a deployment model scenario

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 4 Security threats with Cloud deployment models

The above Table 4 shows the threats associated with three important cloud deployment models, Publix Cloud, Private Cloud, and Hybrid Cloud [105].

In the following Figure 7 cloud computing architecture is shown which contains three service models [106][107]. Figure 8 shows issues and solutions in the service architectures.These servicing models, SaaS, PaaS, IaaS, have security dimensions,

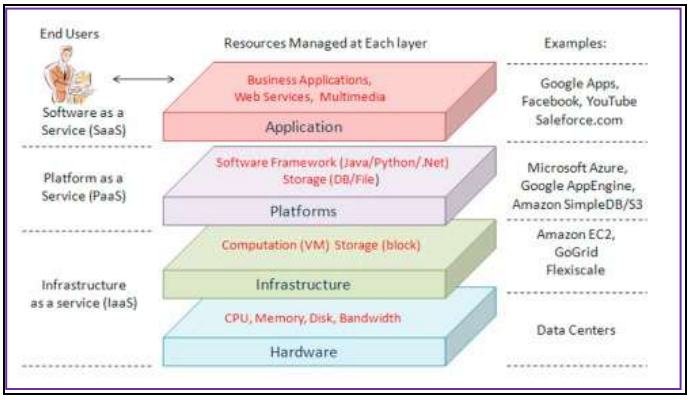

Figure 7 Cloud computing Architecture and its three service models

	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.

Figure 8 Issues of Service Architectures: Issues and Solutions

.	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 modified by the hackers	Active content filtering, Content based data leakage prevention technique, Web application vulnerability detection technique
	Man in middle attack (MIM)		Intruder tries to tap the conversion between sender and receiver	Important data /information may be available to the intruder	Robust encryption tools like Dsniff, Cain, Ettercap, Wsniff and Airjack may 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 other than the intended one	Domain name system security extensions (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 eavesdropping		Malicious insiders and network users	Intruder may get network information and prevent the authentic packets to reach its destination	
Application Layer Attacks	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 authorized user	Intruder may get unauthorized access to a web page or an application of the authorized user	A regular cookie cleanup and encryption of cookie data may prevent this vulnerability
	Captcha Breaking		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 5 Security threats and their solutions in Cloud Computing

The above Table 5 depicts an overview in tabular form cloud threats and their prevention techniques [105] [108]. It covers basic, network, and application threats in cloud environment. Threats which have been discovered but which are continuously expanding along with searches for their prevention when cloud technological innovations are in continual development [109]. As can be guessed and earlier indicated, the above-mentioned Table does not list numerous threats which have been discovered but which continuously expanding along with searches for their prevention when cloud technological innovations are in continual development [109].

Generally the same vulnerabilities, attacks and risks that come from traditional computing are also there in the Cloud Computing although the latter some additional threats emanating from virtualized resources and hypervisor [110]. Moreover, since continual innovations are like to continue, new attacks will continue and this reality must be realized and anticipated [109]. The massive power that CC has is an inducement that may prompt the hacker to launch attacks against users in the same or other networks [111]. Security threats, showing no signs of abatement are fast becoming 'a hot spot' in CC [105]. This is due to the expansion of cyberspace, which is basically due to its constituents such as desktops, laptops, mobiles etc, which are connected to the internet linked to hardware and software. Moreover, IoT and CC platforms have been instrumental to this expansion of cyberspace affording criminals to inflict variety of attacks. What is worthy of note is that 'Some vendors have major focus on their product's quality and minor on cybersecurity. They do not implement the full-fledged cybersecurity mechanisms which give opportunities to the cyber attacker to enter an Internet or network system like an authenticated user. This increased cybersurface gives rise to the difficult level of defending data on the cybersurface by security professionals. Some new type of security standards is needed to implement properly the cybersecurity to save the cyberspace from cybercriminals' [9].Often vendors 'falsely claim to provide secure data and computational environments for cloud users'[83]. Zargari and Smith are quite blunt in respect of users' data breach and loss when they remark that ' there exist various incentives for cloud providers to behave unfaithfully toward the users regarding the status of their data where the users may not retain a local copy of their data. For example, it is possible for the cloud providers to discard occasionally accessed data without being detected in a timely fashion in order to reduce costs and increase the profit margin. In addition, it is also possible for the cloud provider to hide incidents of data loss in order to maintain their reputations' [112]

Quire a number of security deficiencies arise in CC due to many technologies (viz. networks, databases, operating systems, virtualization, resource scheduling, load balancing, etc) which it uses[113]. Naturally, as Samarati and di Vimercati, poignantly states that " security threats can arise 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 – behaviour should be controlled'[80].Take, for instance, the threat of DoS that exists in all servicing models. Alani caustically remarks that there is 'no clearly identified cure' for this. 'In terms of mitigating this threat, there is not much that can be done to prevent it. Being at the receiving end of a DoS attack is analogous to being caught in traffic lock, you

cannot get to your destination and you can do nothing about it except waiting. The service outage becomes very frustrating to clients and they start reconsidering the reasons why they moved their data to the cloud' [114]. Kumar has the same view, saying that 'we believe that no single technology-based solution alone can be effective in providing defence against a variety of DoS attacks. The comprehensive protection of an organization from DoS attack requires a multi-faceted security strategy' [115]. In case security breach there is no single solution to prevent 'since security comes in layers of defences' and new attacks are fired not because of CC is maturing but because enormous data sets can be monetised by application such as advertising [112].There is difficulty in Forensics because 'in the cloud, evidence is likely to be ephemeral and stored on media beyond the immediate control of an investigator [114]. If available, digital evidence as to satisfy the same conventional requirements: it must be authentic, reliable,. Complete, believable and admissible. Further, legal complications may arise if victim, perpetrator and the cloud platform are in within different jurisdictional limits [38]. While discussing network security, Pathy et al. suggest that 'although 'Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems' [113]. Vacca states that computer systems will not be free from vulnerabilities since they are designed, implemented and tested by humans who more prone to making mistakes [110]. Such being the Case there will be newer types of attack incidents resulting from 'unknown vulnerabilities' [116].

It is recommended that cryptographic mechanism – encryption- will safeguard cloud data and its integrity [77]. Singh and Chatterjee thus states that 'bad implementation of the algorithm or uses weak key in the encryption increase possibility of attack. The most common attack in cryptography is brute force attack, match all possible keys with the encryption key in a known range' and they recommend, to protect massive databases, use of Advanced Encryption Standard (AES) and Message Authentication Code (MAC)' [79]. However, Berrezzouq et al. forcefully tend that 'many times in cryptographic mechanisms seem to fail when the security measure applied. In cloud, cryptography applied to overcome the loopholes in security areas but many challenges still exist, so it is important to overcome them. Prime factorization of large numbers in RSA and discrete logarithmic problem in ECC failed for bad password and faulty implementation causes brute force attack. Poor key management, computation efficiency, verifiable data are also other issues related to cloud cryptography' [117]. Veeramachaneni contends that the cryptographic key generation and management for cloud is not standardized and hence 'absence of secure and standard key management techniques for the cloud does not allow the standard cryptographic mechanisms to scale well to the cloud computing model. Therefore, domain of cryptography also enhances the potential risks to the data' [118]. The irony is that criminals also widely use encryption to hide their criminal activity and illegal images [38][8]. What is more, a cyber criminal can open an account in the cloud, which has massive computing power and storage capacity, and then can close the account completely and disappear after having committed a cloud crime leaving no trace whatsoever. The aggravates 'forensic difficulties and challenges in the cloud environment' [38]. A recent development is the emergence of what is called 'dark net' where the drug dealer can sell their goods without face-to-face interaction. With the rise of 'crime-as-service, some programmers who can create the viruses/spam/Trojans/DDoS capabilities' could sell their products to lay persons in the dark net. This is another obstacle to cloud control measures for smooth functioning of the cloud [119].

VI. CONCLUDING REMARKS: UNCERTAINTY AND RISKS DIMENSIONSIN THE TRANSITIONAL ERA OF LIQUID MODERNITY IN THE RISK SOCIETY

Most researcher in CC are more than less unanimous on the impossibility of designing one holistic model or framework for securing Cloud's resources and functionalities. CC risks are overwhelming that persist really or potential in the CC and its different layers. There is no 'single solution' or 'end –to-end security' [112][75]. There is neither 'one technique for all layers' nor 'one silver bullet' for controlling the risks at the network level [9][120]. Samariti and di Vimercati conclude that 'there is not a one-size-fits-all solution (or even a one-size-fits-all problem definition). There are instead different aspects, with related issues, challenges, and security controls that need to be considered and that can find application in different scenarios' [80]. Srinivasan tells that there are nine risks in the CC. 1. Lack of control over the computer infrastructure; 2. Security and controls risk; 3. Risks due to service management by cloud providers; 4. Risks concerning regulatory compliance; 5. Risks caused outage and service unavailability; 6. Risks of data breach; 7. Risks faced by customer because of cloud providers' inability to provide service due to financial or legal difficulties. 8. Risks of data lock-in; and 9. Lack of access to log data [121]. No less important is the arrival of 'speculative-execution attacks such as Meltdown attacks and Spectre attacks that 'exploit computer micro-structural vulnerabilities in modern processors to speculatively execute instructions that steal secrets across security boundaries and transmit them through micro-architectural side channels' [122]. It is now quite understandable in the preceding context why Hasizhume et al. raise the issue of uncertainty surrounding CC security [90]. In fact, in an excellent contribution, Menzi et al. characterized CC as

'the uncertain cloud'. The following Table 6 tells it all [123]. To summarize it in his own words: 'Cloud services often are associated with some uncertainty in their information, including quality of service (QoS) levels, users ratings, available resources, workload and performance changes, dynamic elasticity, availability zones, service descrip-tions, etc. In addition, the highly dynamic cloud environment adds a new factor of uncertainty, as it may have a negative impact on the quality of cloud services and, consequently, on services provisioning and integration. This uncertainty regard-ing the cloud services context raises a question about how to trust the available cloud information and brings additional challenges to the cloud actors.

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

Table 6 Sources and Impact of Uncertainty on Cloud Computing

Therefore, the need to model and handle uncertainty in the context of cloud environments is of 'paramount importance to maintain the sustainable use of such technology' [123]. It thus seems to the present researchers that cloud risks (including, threats and vulnerabilities) have become institutionalized in the industrial capitalist society in the transitional age of liquid modernity. Indeed, both Beck and Giddens, *inter alia*, draw particular attention to the element of risk as an integral constituent part of the social structure [6][124]. Risk, originating in environmental issues triggered predominantly by, among other things, science and technology in the second modernity from the 1970s caught global attention. It became an organising concept 'to reduce the likelihood of harm from myriad ingenious technological activities to levels that are either safe, demonstrably safe , or – if safety is an unattainable goal-then at least to levels that can be shown be reasonable. ... Just as, a century or so ago, the idea of *progress* helped to name an optimistic era, so today *risk*, by its very pervasiveness, seems to be the defining marker of our own less sanguine historical moment' [125]. If risk is technologically embedded in CC, it is also societally embedded as a material cultural component. Simply speaking, cloud risk as a technological risk is also an integral component of social structure of information capitalist or networked society in late – second - modernity in Becks' terms. For him, 'Risk may be defined as a *systematic way of dealing with hazards and insecurities induced and introduced by modernization itself.* Risks, as opposed to older dangers, are consequences which relate to the threatening force of modernization and to its globalization of doubt. They are *politically reflexive*... The diffusion and commercialization of risks do not break with the logic of capitalist development completely, but instead they raise the latter to a new stage. There are always losers but also winners in risk definitions. The space between them varies in relation to different issues and power differentials. Modernization risks from the winners' points of view are *big business*' [6]. Risk society is a *catastrophic* society where one can possess wealth but they also can be *afflicted* by risk which is *invisible*. Risks strengthen but does not abolish class society though poverty attracts plenty risks whereas the wealthy with income, power or education can purchase safety and avoid risk which has *inherent tendency towards globalization.* Risks have a *boomerang effect* in the sense that risk catch with those who produced or profit by them. Risks, which generate social differentiation (abolitions or creation of work hierarchies) and conflicts, have a double face: 'risks 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. The social and economic importance of *knowledge* grows similarly, and with it the power over the media to structure knowledge (science and research) and disseminate it (mass media). The risk society is in this sense also the *science, media and information* society. Thus new antagonisms open up between those who *produce* risk definitions and those who *consume* them' [6].

How does Beck rate risk in techno-scientific terms? Here is what is says in quote: 'Today's recognized knowledge of the risks and threats of techno-scientific civilization has only been able to become established *against the*

massive denials, against the often bitter resistance of a self-satisfied 'techno-scientific rationality' that was trapped in a narrow-minded belief in progress. The scientific investigation of risks everywhere is limping along behind the social critique of the industrial system from the perspectives of the environment, progress and culture. In this sense, there is always a good bit of the unavowed cultural *critical zeal of a convert* in the techno-scientific concern with risks, and *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 to Lutheranism*. … Techno-scientific development is beginning to be trapped more and more within a striking new contradiction: while the foundations of knowledge are being explored in the institutionalized self-scepticism of the sciences, the development of technology has been isolated against scepticism. Just as the risks and the pressure for action grow, absolutist claims to knowledge, infallibility and security, which have long since become untenable, are being renewed in technological development. Dogma flourishes under the pressure on the *engineering sciences* to take action. The unleashed and systematically fomented scepticism encounters the *anti-modernity* of scientific infallibility taboos in the development of technology. These harden as the risks increase' [6]. Furthermore like CC, risk society has become globalized in the with limited controllability of the dangers o f our creation, demanding decisions under conditions of 'manufactured uncertainty'. Hence, 'enabled by the information revolution, global market risk allows the near-instant flow of funds to determine who, if any one will prosper, and who will suffer' [126]. But to be sure, Beck was no pessimist. He reminds us that risks, which cannot be banned altogether, should be tackled with new institutional arrangements. But it is not with the idea in mind that we might be able to gain full control, but much more with the idea in mind that we have 'to find ways to deal democratically with the ambivalences of modern life and decide democratically which risks we want to take'[126].

This call for democratization also applies to CC which has crossed many hurdles to become another utility in the IT system, just as electricity, telephone or water have become. Sultan argues for democratization of this CC as disruptive innovation and concludes that 'if democracy is about empowering the weak by providing equal access to resources then cloud computing is emerging as a democratizing force. It has the potential to provide less-endowed SMEs with access to resources that would have been outside their affordable reach' and it does have 'the potential to bridge the digital divide that exists between developed and developing countries' [127]. This is of course not an accidental assertion. Stark and Tierney, while reporting on an empirical research on an encrypted cloud storage application called Lockbox, voiced the same opinion. Arguing that CC storage as a 'technological innovation is by no means neutral' and call for embodiment of values (e.g. user autonomy, privacy, usability, and cost) in CC. Since human life cannot be usefully bifurcated online and offline components, 'designers of laws and devices should begin their legal and technical work with a commitment to investigate core democratic values such as freedom or privacy, and construct online norms consistent with these values, reinforcing ''moral imperatives'' stemming from values such as user autonomy, as opposed to technological imperatives stemming or subsumed values of a less democratic bent' [128].

Pursuing further the comparison between risks of CC and those of present day society in which the former are embedded, Giddens, unlike Beck, considers that risk is not the same as hazard or danger. For him, risks refer to hazards that are 'actively assessed in relation to future possibilities'. They appear, as in present times of transitional modernity, only when society becomes 'future oriented' and actively wants 'to break away from its past—the prime characteristics of, indeed, modern industrial civilization'**.** The concept of risk is inseparable from the from the ideas of 'probability and uncertainty' and no one can be said to run a risk 'where an outcome is 100 per cent certain' [124]. Risk is not merely a negative notion but is ' a mobilising dynamic of society that bent on change, that wants to determine its own future (and also safety) rather than leaving it to religion, tradition or the vagaries of nature'. This explains why capitalism is dynamic compared with earlier forms of economic system. Echoing Beck, Giddens says that 'modern capitalism embeds itself into the future by calculating future profit and loss, and therefore risk, as a continuous process' [124]. There are two types risk. The first is unexpected external risk which persisted till the end of tradition or till the pre-modern era. The second risk is 'manufactured risk' to which Beck also referred. For Giddens, risk society is a society which is 'increasingly preoccupied with the future (and also with safety), which generates the notion of risk', and it is especially the progress of science and technology that created 'manufactured risk' in course of the very progression of human development. While political implications and new institutional arrangement are required [129], as Beck reminded, Giddens emphasizes positive dimensions of risk. As he says, 'there can be no question of merely taking a negative attitude towards risk. Risk always needs 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 innovation or other forms of change. After all, one root of the term 'risk' in the original Portuguese means to 'dare'' [124]. All this sounds like urgently facing the challenges of CC and its security countermeasures, even when they are integral component of the contemporary risk society in the positive sense.

It is thus understandable why worldwide public cloud revenue will grow from 182.4 in 2018, to 249.8 in 2010 to 331.2 billion US dollars, according to Gartner forecast [130]. 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' [131]. CC 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 it 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' [132]. Buckholts et al. show how the globalization of world economy created cloud manufacturing which is defined as manufacturing focused on providing services-based on resources from its pool virtualized manufacturing material: service can be provided through the IoT in order to have easy access'[139].

In the present context, as Winter et al. rightly elaborate the relationship between the social and technological, by saying that this relationship is 'not limited to technology impacting the social realm—they are mutually arising phenomena, enmeshed with sociocultural, political, economic, or scientific aspects' [133]. As far as CC and its relationships to the risk society are concerned, the message of risk society is that industrial societies both manufacture but must also control risk too. 'Risks are not just moments of danger as we forge forward: they are the process itself' [134].The distinctive lesson from the interdisciplinary futuristic perspective is that 'it values and tries to *understand* the uncertainty of the future. Acknowledging the inherent uncertainty of the future helps us to expand our ideas about the unknown future. If we stick to and only value certainty, our options and choices end up very narrow. If we are open to uncertainty, though, we become open to various possibilities in the future.'[133]

REFERNCES

[1] Giddens, A. (1996). The Consequences of Modernity, Cambridge, Polity Press, pp. 7, 10.

[2] Bauman, Z.(2008). Liquid Times Living in an Age of Uncertainty, Cambridge, Polity Press, p. 1.

[3] Bauman, Z. (2006). Liquid Modernity, Cambridge, Polity Press.

[4] Giddens, A. (2006). Modernity and Self-Identity, California, Stanford University press, p. 3.

[5] Beck, U. (1996). Risk Society: towards a New Modernity, London, Sage, p.19, 21, 23-5, 26, 45,158, 177.

[6] Devi, S. and Rather, M.A. (2019), 'Cyberspace and Cyber Security in the Digital Age: An Evolving Concern in Contemporary Discourse', in (eds.) B.R Gupta, D.P. Agrawal, and H. Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, New York: CRC Press, p. 96.

[7] Archibugi, D. and Pietrobelli, C. (2003), 'The globalization of Technology and its Implications for Developing Countries: Windows of Opportunity or Further Burden', Technological Forecasting & Social Change, 70, p.865.

[8] Vincze, E.A. (2016), 'Challenges in Digital Forensics', Police Practice and Research, 17(2), p. 187-8.

[9] 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, pp. 1-2, 9.

[10] Zaharia, M.H. (2014), 'A Paradigm Shift in Cyberspace Security', in (eds.) B. Akhgar and H.R. Arabnia, Emerging Trends in ICT Security, Amsterdam: Elsevier, p. 443.

[11] Bell, D. et al (eds.), (2004), Cyberculture: the Key Concepts, Rutledge: London, p. 42.

[12] Dodge, M. and Rob Kitchin, Mapping Cyberspace (2001), Rutledge: London, p.1.

[13] Whittaker, J. (2004), The Cyberspace Handbook, Rutledge: London, p. 5.

[14] Wittel, A. (2001), "Toward a Network Sociality', Theory, Culture & Society, 18(6), p. 51.

[15] Lash, S., and J. Urry (1994), Economies of Signs and Space, Sage: London, p. 252.

[16] Castells, M. (200), 'Materials for an Exploratory Theory of the Network Society', British Journal of Society, 51(1), pp.5-24.

[17] Nielsen, S.C.(2012), 'Pursuing Security in Cyberspace: Strategic

and Organizational Challenges', Orbis (Summer), doi: 10.1016/j.orbis.2012.05.004, pp. 337-40.

[18] Cybersecurity Ventures (2019). 2019 Official Annual Cyber Crime Report-HerJavek Group, https://www.google.com/search?source=hp&ei=8xAYXryOCaLWz7sPvriYiA4&q=2019+official+annual+cybercrime+report&oq=2019+official&gs_l=psy-ab.1.2.0l10.3931.12945..18905...0.0..0.241.2430.0j13j1....2..0....1..gws-wiz.....6..0i362i308i154i357j0i131.-WwhpfTp2Os. [Accessed on 01 January, 2020].

[19] Fields, Z. (2018), Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution, IGI Global: PA, USA, p. 113.

[20] Easttom, C. and D. J. Taylor (2011), Computer Crime, Investigation and the Law, Course Technology: Boston, pp. 43, 49-50.

[21] Li, J., and F. Fawzl (2017), Research About Attacks over Cloud Environment, International Journal of Scientific & Technology Research, 6(1), p.7.

[22] Bernik, I. (2014), Cybercrime and Cyberwarfare, ISTE Ltd : London, p. 5'

[23] Norton by Symantec, (2018), 2017 Norton Cyber Security Insights Report Global Results, https://www.google.com/search?source=hp&ei=v5QYXrGxEs_Zz7sP986I8Ag&q=2017+Norton+Cyber+Security+Insights+Report+++Global+Results%2C+&oq=2017+Norton+Cyber+Security+Insights+Report+++Global+Results%2C+&gs_l=psy-ab.12..0i22i30.1709537.1709537..1713833...0.0..0.244.408.0j1j1....2..0....2j1..gws-wiz.....6..0i362i308i154i357.2zZfDvy9TXI&ved=0ahUKEwjxjNCdqfnmAhXP7HMBHXcnAo4Q4dUDCAk . [Accessed on 01 January,2020].

[24] Chang, J., FinancesOnline (2020). https://financesonline.com/cybersecurity-statistics/. [Accessed on 01 January 2020]

[25] Sobers, R. (2019), 110 Must-Know Cybersecurity Statistics for 2020, https://www.varonis.com/blog/cybersecurity-statistics/. [Accessed 01 January 2020.

[26] Hill, J.B., and N.E. Marion (216), Introduction to cybercrime : computer crimes, laws, and policing in the 21st century, Praeger: California, p. 4,5-6.

[27] 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.

[28] Brenner, S.W. (2010], Cybercrime: criminal threats from cyberspace, Praeger: California, p. 10.23, 36.

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

[30] Willems, E. (2019), Cyberdanger: Understanding and Guarding Against Cybercrime, Springer: Switzerland, p. 187.

[31] Sen. J. (2013]. 'Security and Privacy Issues in Cloud Computing', Xvi:1303.4814v[CR], p.8.

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

[33] von Holms. B.,(2000), 'Information Security-The Third wave', Computers and Security', 19 (2000), pp.615-6.

[34] 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.

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

[36] von Solms, R., and J. van Niekerk, (2013), 'From Information Society to Cyber Security', Computers& Security, 38, pp. 97-102.

[37] 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.

[38] Pichan, A., et al. (2015), 'Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis, Digital Investigation, 12, pp. 52-4.

[39] 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.

[40] Da Veiga and N. Martins (2017), 'Defining and Identifying Dominant Information Security Cultures and Subcultures', Computers & security, 70, 72-94.

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

[41] 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.

[42] Angraini. et al.(2019), 'Information Security Policy Compliance: Systematic Literature Review', Procedia Computer Science, 161, pp. 1216-24.

[43] Paananen, H. et al.(2020), ' State of Art in Information Security policy Development', Computer & security, 88, pp. 1-14.

[44] Renaud, K., et al. (2018), 'Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious?', Computer Security, 78, p.207.

[45] 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.

[46] Bhowmik, S. (2017), Cloud Computing, Cambridge University Press: Cambridge, p. 272.

[47] Dahbur, k., et al.(2011), ACM 978-1-4503-0475-0/04/2011, p. 3.

[48] Tonhauser, M, and J. Ristvej (2019), 'Disruptive acts in Cyberspace, Steps to Improve Cyber Resilience at National Level', Transportation Research Precede, 30. p.1591.

[49] 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.

[50] 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. 196-7.

[51] Huang, K. and K. Pearlson, '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.

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

[53] Yildirim, E. (2016), 'The Importance of Information Security Awareness for the Success of Business Enterprises', in (ed.), Nicholson, D. ,Advances in Human Factors in Cybersecurity, Springer Nature: Switzerland, pp. 212-3.

[54] Thomson, K-L. (2006), 'Cultivating an Organizational Information Security Culture, Computer Fraud & Security, (October 2006), p. 7.

[55] Simmonds, M.(2018), 'Instilling a Culture of Data Security Throughout the Organization', Network Security, (June 2018),pp. 9-10.

[56] Patterson, W. et al. (2016), 'Behavioral Cybersecurity: Human Factors in the Cybersecurity Curriculum' in (ed.), Nicholson, D., Advances in Human Factors in Cybersecurity, Springer Nature: Switzerland, pp.257-8.

[57]Tischler, H.L.(2011), Introduction to Sociology, Wadsworth: California, pp. 4, 51, 54-5, 104.

[58] Frangopoulos, E.D. et al. (2008), 'Social Aspects Of Information Security' https://www.researchgate.net/publication/220803394_Social_Aspects_of_Information_Security/link/00b7d537b0845f3f5c000000/download, DBLP Conference Paper, January 2008, pp. 1-33.

[59]Li, et al.(2019), 'Investigating the Impact of Cybersecurity policy Awareness on Employees' Bevaiour', International Journal of Information Management, 45, pp. 13-24.

[60] Lim, J.S., et al. (2009), 'Exploring the Relationship between Organizational Culture and Information Security Culture', Proceedings of the7th Australian Information Security Management Conference, 2009, DOI: 10.3225/75/576/40665130def., pp. 88-97.

[61]De Veiga, A., and N. Martins, 'Information Security Culture and Information Protection Culture: A Validated Assessment Instrument', Computer Law & Security Review, 31, pp. 243-56.

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

[63] ENISA, Cyber Security Culture in Organizations (2017), ENISA: Greece, p.7.

[64] 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.

[65] De Vega, A., and Eloff, J.H.P. (2010), ' A framework and assessment instrument for information security culture', Computers & Security, 29, pp.197.

[61]De Vega and N. Martin (2015), 'Information security culture and information protection culture: A validated assessment instrument', Computer Law & Security Review, 31, p. 249.

[66]Nasir, A., et al (2019), ' An analysis on the dimensions of information security culture concept: A review', Journal of Information Security and Applications, 44, pp.14-6, 19.

[67] van Niekerk and R. von Solms , 'Understanding Information Security Culture: A Conceptual Framework, https://www.researchgate.net/publication/220803272_Understanding_Information_Security_Culture_A_Conceptual_Framework/link/0deec51909305545d0000000/download, [Accessed on 15 December 2019]

[68] Glaspie, H.W., and Karwowsaki (2018), 'Human Factors in Information Security Culture: A Literature Review', in (eds.), Nicholson, Advances in Human Factors in Cybersecurity, Springer: Switzerland, p. 271.

[69] Angrani et al.(2019), 'Information Security Policy Compliance: Systematic Literature Review', Procedia Computer Science, 161, p. 1261.

[70] Paananen, H. et al., (2020), State of the Art in Information Security Policy', Computer & Security, 88, p. 1.

[71] General Assembly. United Nations.Resolution adopted by the General Assembly A/RES 57/239. Creation of a global culture of cybersecurity, https://www.itu.int/ITUD/ cyb/cybersecurity/docs/UN_resolution_57_239.pdf. [Accessed 10 December 2016].

[72] Wall, D.S., (2017), 'Towards a Conceptualization of Cloud(Cyber)Crime', in (ed.), T. Tryfonas, Human Aspects of Information Security, Privacy and Trust, Springer: Switzsrland, p. 53345

[73] Stark, L., and M. Tierney (2014), 'Lockbox: Mobility, Privacy and Values in Cloud Storage', Ethics and Information Technology , 16(1), p. 1.

[74] 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. 293.

[75] Mehra, N. et al (2018), 'Analysing Cloud Computing Security Issues and Challenges', in Pattnaik, P.K., et al.,(eds.), Progress in Computing Analytics and Networking, Springer: Switzerland,

[76] Iqbal, S. et al.(2016), ' On cloud security attacks: A taxonomy and intrusion detection and prevention as a service', Journal of Network and Computer Applications, 74, pp.112-17

[77] Bennasar, H. et al. (2017), 'An Overview of the State-of-the-Art of Cloud Computing Cyber-Security, (eds.) S.E. Haji, et al., Codes, Cryptology and Information Security: Second International Conference, C2SI 2017, pp. 60—61.

[78] Coppolino, L. et al.(2017), ' Cloud security: Emerging threats and current solutions', Computers and Electrical Engineering, 59, p.127.

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

[80] Samarati, S.D. and Di Vimercati.(2016), 'Cloud Security: Issues and Concerns'. in (eds.) ,S. Murugesan and I. Bojanova, Encyclopaedia of Cloud Computing, Wiley: UK, p. 2017.210.

[81] Ali M. et al(eds.), ' Security in Cloud Computing: Opportunities and Challenges', Information Science, 305, p. 361.

[82] Fernandes, D.A.B., et al.,(2014), 'Security Issues in Cloud Computing Environments', International Journal of Information Security, 13, pp.117-22.

[83] Khalil, I.M. et al.(2014), 'Cloud Computing Security: A Survey', Computers, 3, pp. 6. 26.

[84] Zissis, D. and D. Lekkas (2012), 'Addressing Cloud Computing Security', Future Generation Computer Systems', 28, p. 587.

[85] Subashini, S, and V. Kavitha, 'A Survey on Security Issues in Service Delivery Models of Cloud Computing' Journal of Network and Computer Applications, 8, p. 4.

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

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

[88] 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.

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

[90] Hashizume, K., et al.(2013), 'An Analysis of Security Issues for Cloud Computing', Journal of Internet Services and Applications', 4-5, pp. 1, 6.

[91] 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.

[92]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.

[93] Sultan and van de Bunt-Kokhuis (2012),'Organizational Culture and Cloud Computing: Coping with a Disruptive Innovation', 'Technology Analysis& Strategic Management', 24(2), p. 173.

[94] 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, p. 132.

[95] 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.

[96] Singh, S. et al. (2016), 'A Survey of Cloud Computing Security: Issues, Threats, and Solutions', 'Journal of Network and Computer Applications', 75, p. 204.

[97] 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.

[98] Kumar, R. and R. Goyal (2019), 'On Cloud Security Requirements, Threats, Vulnerabilities and Countermeasures: A Survey', Computer Science Review, 33, pp. 11-31.

[99] 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.

[100] Modi, C. et al. (2013), A Survey on Security Issues and Solutions at Different Layers of Cloud Computing', Journal of Supercomputer, 63, pp. 561-93.

[101] 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.

[102] 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.

[103] 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.

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

[105] Deshpande, P.S., et al. (2019), Security and Data Storage Aspect in Cloud Computing, Springer Nature: Singapore, pp. 7, 9-10.

[106] Parikh, S., et al., (2019), 'Security and Privacy Issues in Cloud, Fog and Edge Computing', Procedia Computer Science, 160, p.735.

[107] Singh, P., and E.A. Jain (2014), 'Survey Paper on Cloud Computing', International Journal of Innovations in Engineering and Technology (IJIET), 3(4), p.85.

[108] Akshaya, M.S. et al., (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.

[109] Maniah, et al.(2019), 'Survey on Threats and Risks in the Cloud Computing Environment', Procedia Computer Science,161, p. 1332.

[110] Oliveira et al., 'Cloud Security Baselines' in (ed.),J.R. Vacca, Cloud Computing Security: Foundations and Challenges, CRC Press: London, 2017, p.43.

[111]Chou. T.S, (2013),'Security Threats on Cloud Computing Vulnerabilities', International Journal of Computer Science & Information Technology(IJCSIT), 5(3), p. 87.

[112] Zargar, S.A. and A. Smith (2014), 'Policing as a Service in the Cloud', Information Security Journal, 23(4-6), pp.154, 156.

[113] Padhy, R.P., et al.(2011), 'Cloud Computing: Security Issues and Research Challenges. 'International Journal of Computer Science and Information Technology & Security' (IJCSITS), 1(2), p.136.

[114] Alani, M. A.(2016), 'Elements of Cloud Computing Security'. Springer: Switzerland, p. 31.

[115]Kumar, G. (2016), 'Denial of Service Attacks – an updated perspective', System Science & Control Engineering, 4, p. 294.

[116]Hong, J.B. et al. (2019), 'Systematic Identification of Threats in the Cloud: A Survey', Computer Networks,, 150, p. 66.

[117] Beerezzouq, M. et al., (2019), 'Issues and Threats of Cloud Data Storage', in (eds.), Zbakh et al., Cloud Computing and Big Data: Technologies, Applications and Security, Springer: Switzerland, p.62.

[118] Veeramachaneni, V.K.(2015), ' Security Issues and Countermeasures in Cloud Computing Environment '. International Journal of Engineering Science and Innovative Technology (IJESIT), 4(5), p. 87.

[119] Warren, S., et al. (2017), 'How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?', in (ed.), T. Tryfonas, Human Aspects of Information Security, Privacy and Trust, Springer: Switzerland, p.541.

[120] Chaka, J.G, and M. Marimuthu, 'Curtailing the Threats to Cloud Computing in the Fourth Industrial Revolution' in (ed.), Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution', IGI Global: PA, USA, p. 135.

[121] Srinivasan, S. (2014), Springer: New York, 29-37,107-10.

[122] Zhang, Y., and Sion, R. (2019), 'Speculative Execution Attacks and Cloud Security'. ACM ISBN 978-1-4503-6826-1/19/11, https://doi.org/10.1145/3338466.3360287, p. 211.

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

[124] Giddens, A.(2002), Runaway World, Profile Books: London. No paging.

[125] Jasanoff, S.(1999), 'The Songliness of Risk', Environmental Values, 8, pp. 135-6.

[126] Beck, U. (1999), World Risk Society, Polity Press: London.

[127] Sultan, N. (2013), 'Cloud Computing: A Democratizing Force?', International Journal of Information Management, 33, p.814.

[128]Stark, L., and M. Tierney (2014), 'Lockbox: mobility, privacy and values in cloud storage, Ethics and Information Technology', 16, p. 11.

[129] Giddens, A. (1999), 'Risk and Responsibility', The Modern Law Review, 62(1), pp. 3-5.

[130]Gartner. (2019), Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g [Accessed on 07 January 2020), p. 1.

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

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

[133] Winter J., and R. Ono (2015), 'Introduction to the Future Internet: Alternative Visions' in (eds.), J. Winter and R. Ono, The Future Internet: Alternative Visions, p. 9.

[134] Woollacott, M.(1998), 'Risky Business Safety', in (ed.) J. Franklin, The Politics of Risk Society , Polity: Cambridge, p. 49.

[135] Mell, P. and T. Grance (2011), 'The NIST Definition of Cloud Computing: NIST: Special Publication 800-145', Computer Security Division: MD 20899-8930, p. 2.

[136] Dataflair Team (2019), 'Features of Cloud Computing – 10 Major Characteristics of Cloud Computing', https://data-flair.training/blogs/features-of-cloud-computing/ [Accessed on 12 December 2019].

[137] 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.

[138]Mukhiya, S.K,(2015,'Cloud computing, Software Architecture, https://study-for-exam.blogspot.com/2015/06/explain-cloud-computing-deployment-model.html [Accessed on 20 December 2019].

[139] Buskholts et al. (2015), 'Cloud Manufacturing: Current Trends and Future Implementations', Journal of Manufacturing Science and Engineering, 137, p. 040902-1.

Acknowledgement:

I gratefully acknowledge the assistance I received from Retired Professor, Bipul Kumar Bhadra, PhD (McMaster), of Jadavpur University in Kolkata.