Emerging Trends in Cloud Computing, Big Data, Fog Computing, IoT, and Smart Living

Amin Hosseinian-Far[1], Muthu Ramachandran[2], Charlotte Lilly Slack[3]

School of Computing, Creative Technologies & Engineering, Leeds Beckett University, Leeds, UK

{[1]A.Hosseinian-Far, [2]M.Ramachandran}@leedsbeckett.ac.uk;
[3]lillyslack@hotmail.co.uk

Keywords: Cloud Service, Big Data, IoT, Smart City

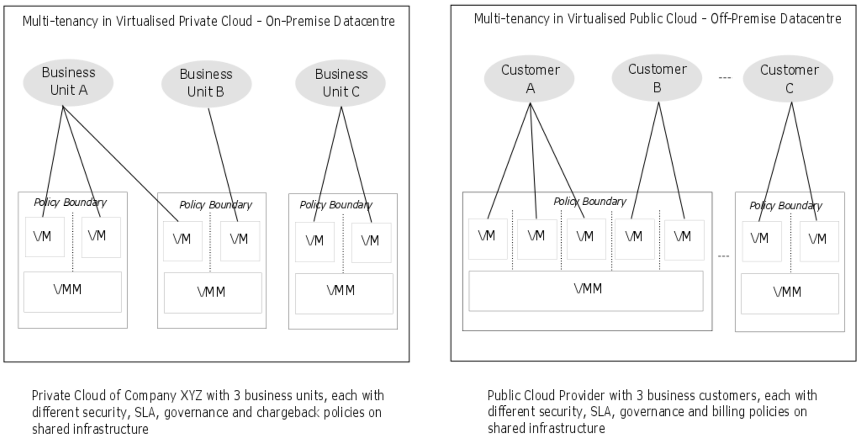
Abstract. Cloud computing has emerged to address the needs of businesses and to improve the quantity and quality of data that we can collect and analyse from multiple sources and devices. Cloud computing has also revolutionised the software paradigm by changing into a service-oriented paradigm where cloud resources and software are offered as a service. This service archetype has changed the way we have been thinking when producing a cloud service. This chapter provides an outline of the underpinning definition, principles, and concepts

which currently lack in the literature. This chapter will also outline the foundations of cloud computing, and then endeavours to draft the emerging trends and evolution of cloud applications. The emerging trends will include new services, federations of cloud paradigm, smart cities, big data, IoT, and mobile cloud.

1. Introduction

There can be many definitions towards the explanation and delivery that Cloud computing has on the impact of the current 21st century generation, too many for anyone to have achieved a rigorous meaning. According to Babcock [1], the ‘Cloud’ is mostly specified and put into the software category labelled as a service, where a software application can be accessed online, at free hand. The main challenge to defining cloud computing is because much like other descriptive buzzwords within the technology industry, there can be many definitions to each individual or firm. Cloud computing provides ‘ubiquitous’, ‘convenient’, and ‘on-demand’ access to a networked and common group of configurable computing assets argued by Samani, et al. [2]. “*As of now, computer networks are still in their infancy. But as they grow up and become more sophisticated, we will probably see the spread of ‘computer utilities’ which, like present electric and telephone utilities, will service individual homes and offices across the country*” [3]. This concept by Leonard Kleinrock in 1969, was the familiar quote that inspired the development of the internet today. Also, dating back to 1960, John McCarthy referenced that “computation may someday be organized as a public utility”, defining what is today the ‘Cloud’ [4]. Armbrust, et al. state that “Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacentres that provide these services” [5]. Compared to the types of services involved in Cloud, and its overall commitment Dhar (2012) gives the most defined yet infonaut definition. Dhar (2012) states, “*Cloud Computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over web browsers and the Internet*” [6]. Cloud

Computing has many benefits and concepts from the Web 2.0, offering Infrastructure as its service [7].


Multi-tenancy in Virtualised Private Cloud - On-Premise Datacentre
Business Unit A
Business Unit B
Business Unit C
Policy Boundary
VM
VMM
Multi-tenancy in Virtualised Public Cloud - Off-Premise Datacentre
Customer A
Customer B
Customer C
Policy Boundary
VM
VMM

Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure

Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Figure 1: Multitenancy (adapted from [8])

Figure 1. outlines the concept of multitenancy within cloud computing environments [8]. The notion of multitenancy is simply referring to resource sharing within the cloud environment. In the first rectangle on the left, this resource sharing is illustrated as an example for a private cloud environment in a schematic way. On right, this resource sharing is presented in a public cloud environment. Multitencancy in public cloud can be considered as one of the major barriers for expansion of cloud computing due to existing security risks [9]. Risks such as losing privacy and/or integrity in public cloud may prevent many decision makers to authorise the implementation of digital services using cloud computing in a smart city.

2. Cloud Models

2Cloud computing provides a three types of services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). This section will look at each of these services.

2.1. Service Models

Due to the continuous evolution of the cloud, several cloud models have come to exist to keep up with the market demand and the internet's continuous evolution. In the National Institute of Standards and Technology (NIST), Mell & Grance (2011) has defined three different service models [10]:

Cloud Software as a Service (SaaS) - SaaS has an offer to applications that are provided on their cloud infrastructure [11]. Overall, accountability and managerial organization is ran by SaaS, operating the applications too. The user is responsible of managing the app settings.

Cloud Platform as a Service (PaaS) – PaaS offers a structure to position apps that are already past the development stage, using certain programming supported for the PaaS. As stated before, and by Mell & Grance, the responsibility is upon the SaaS, who do not have control over the users' settings and apps. The user is again responsible for the settings and configurations [11].

Cloud Infrastructure as a Service (IaaS) – IaaS provides the correct resources and tools to suit the users system and app. The user has a responsibility of their operating system, storage, and apps and network configurations [10].

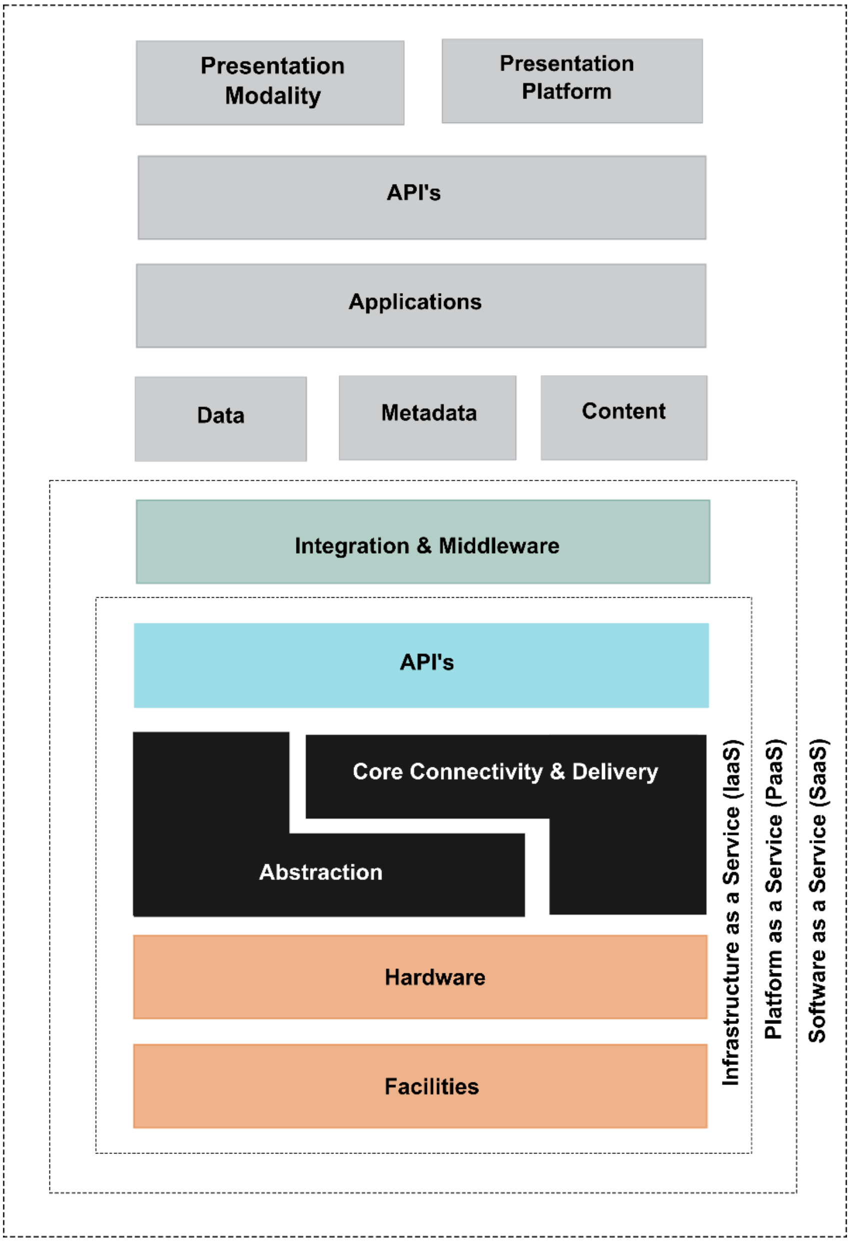


Figure 2: Service Models (adapted from [8])

The three indicated service models allow the use of multi-tenancy environment, apart from when the IaaS model is in use as the users are in total control over responsibility (See Figure 2. for a detailed illustration of the details).

The Software as a Service category is mainly comprised of the API's, Applications, Data and the required presentation platform for the software on the cloud. This would sit on the Platform as Service where, the platform for hosting the software is offered as a service within the cloud environment. Lastly, there is the Infrastructure as a Service which is comprised of the necessary hardware, facilities and the associated protocols.

2.2. Deployment Models

There are several deployment models available in regards to the Cloud today, and more and more will develop as the Cloud technicalities expand [11]. The models stated below are the current models involved in Cloud services so far, and can be used with any of the service models listed above (SaaS, PaaS, or IaaS) [11].

Public Cloud - lWhen discussing the topic of cloud, it is often specified, and reference to as ‘the public cloud’. This is due to the most well-known and popular cloud services being open to the public eye [2]. These service examples include e-mail services, such as, Hotmail, Apple iCloud, or the popular storage services, such as Dropbox. All of these Cloud services are made available to the public, who can access the services via the internet. Whilst many of the general public customers from a particular firm may use a ‘Public Cloud’ service, the nature of the public model will mean that it is available to any individual customer [2].

Private Cloud - Whilst the Public Cloud uses a substructure for several customers, the defined ‘Private Cloud’ is reserved to one individual person, a single customer. Whether the infrastructure of the firm is on sight, or off sight, the individual client will be the only one with access and control to its location and placing [2]. Only one organization constructs within their personal Cloud [11]. Operated in the ‘Private Cloud’ is only information that will be, or is regulated and controlled, such as, personal information and data that should not be duplicated or repeated outside of this cloud. It is a preferred model for hosting private data where restrictions and boundaries can be applied. In comparison to the ‘Public Cloud’ and ‘Community Cloud’ (See below and Fig. 3), a Private Cloud can be ‘trusted’ with limited access [2].

Community Cloud - A Community Cloud extends the concept of a Private Cloud, to allow multiple known members to incorporate into shared concerns in the private cloud. The community of this particular cloud is multiple stakeholders, with similar goals or the same preferences for security and through the whole party, these stakeholders are provided and granted the same data access [2]. The members in the cloud may wish to review those looking and seeking entry in their cloud community [12]. The community cloud may be organized, and managed by the firms, or outsourced to a third party [11]. In a busy cloud market position, many cloud service providers can differentiate themselves better using ‘community cloud’ [13] (See Fig. 3).

Hybrid Cloud - In between the original ‘Private’ and ‘Public’ Cloud, without contrast to the ‘Community’ Cloud, is the ‘Hybrid’ Cloud. The ‘Hybrid Cloud’ is designed to prepare for the implementations that are in between the Public and Private Cloud [2]. The Hybrid is an integrated cloud service, which can utilize the Private and Public to perform the different functions that are needed within the community of the firm [14]. The Hybrid cloud involves several different cloud infrastructures, with different deployment models combined [11].

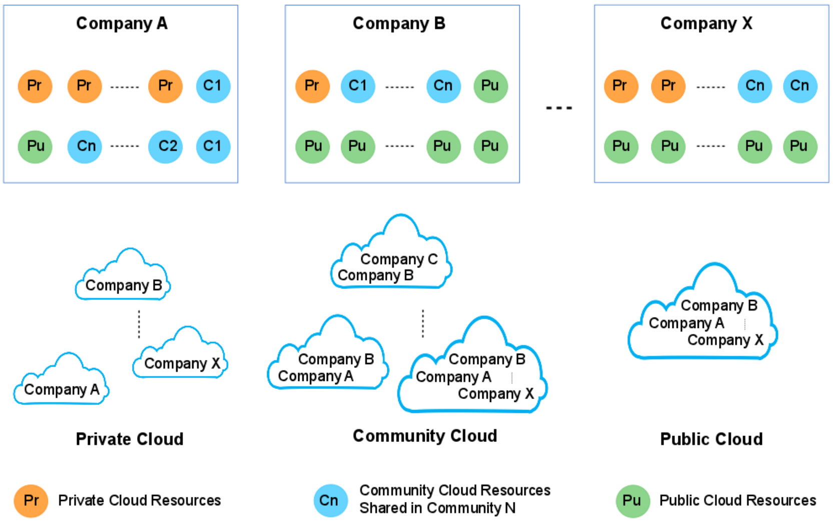


Figure 3: Disparate Resource-Sharing Requirements in Different Companies (adapted from *[15]*)

As discussed earlier in this chapter, resource sharing is one of the objectives of cloud computing as it would benefit storage, processing and manipulation of data across shared resources. However, security, privacy and integrity of the data in a public cloud is often concerning for many decision makers. The public cloud is the desired and relevant deployment model that can be used in a smart city, nonetheless appropriate strategies should be arranged for maximising data security, privacy and integrity.

3. Cloud Services

The Cloud services today have many providers, which are familiar with the common public, including Dropbox, iCloud and Google. All these Cloud services involve various services, where files and information are kept on their servers, which are connected to the internet. Therefore, instead of having to keep them on a single computer, you can use any online device to access the same files. This is useful for the day-to-day business concept of having your important data backed up, and having easy access anywhere to ‘The Cloud’. With the security aspect for the product, the security of these services plays an important role in the development of software systems, such as the Cloud. Security requirement is often considered after the design of the system, which is shown by an analysis of software development processes [16].

3.1. Security and Compliance

Some of the most important concerns in Cloud Computing, are Security and Privacy issues [17]. Throughout the use of the Cloud, there is a constant need for large amounts of personal data, and sensitive data is also managed in the process. The Security concepts, and the privacy image of the Cloud is among the primary reasoning for the Clouds existence, as several surveys state. For different firms, it is essential that the analysis and concept of the security and privacy issues that adopt the cloud-computing infrastructure are understood, before its adoption into business culture [17].

The Cloud service is based on the storage of personal and sensitive information, and the safety of its data, which raises concerns as to whether the Cloud context can be trusted. Many industries for solutions have made sure to take into account the understanding of organizational structures, and laws and regulations that are bound around the social aspects of the situation. When a firm participates into the Cloud IT infrastructure, their data and important documentation is then stored in a different environment, which is managed, and maintained externally to their organization. From this there is a sudden feel of lack of control within the organization. The organization is appropriately giving up their administrative control and processes. Therefore, with respect to the security of the cloud, the consideration of elements including data integrity, data transfer and recovery should be revised [17].

Considering the Cloud Security Landscape, if overall there becomes a failure to ensure appropriate security and safety when the cloud services are in use, this could result in higher costs, and potential loss of business [18]. Thus, disregarding any potential benefits that cloud computing can have on these specific measures for the firm [18]. If the consideration in a firm is to move to the cloud computing process, the stakeholders, including customers, must have a clear mentality and approach [18]. They also need to understand the probable security benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider [18].

3.2. Cloud Security Controls

Cloud Security and its procedures can only be effective if the right security measures are in place and implemented correctly. The Security Management of the cloud service should be in place according to the Cloud architecture that provides the control of the service. With the precise Security Management in place, the Security controls can then be used, and identified to prevent any issues from occurring. These individual controls can be put into place to avoid any flaws, and reduce the chance of an attack on the systems. An example would be a Logon warning, which ensures the person is aware of the right to enter the information storage and the Cloud Storage site [19]. The cloud security controls are the key pillars of Cloud Security [20].

Deterrent Controls- Deterrent controls are measures to diminish any sort of attacks that may occur when on Cloud architecture [21]. An example of this could be a warning sign on a housing property, or a pop up on an IT structure, suggesting further action should be proposed when using software. These are the same as Deterrent Controls, stating there will be opposing concerns and consequences if they were to proceed [19].

Preventive Controls- Preventive controls ensure that any security issues that will intendedly arise, will have already been approached. With the managing of certain issues, damage can then be limited [19]. An example of this would be the proxy server. The preventative acts as a ‘bouncer’ personality between your information, and the person wanting to access it. On request for this information, it can be granted and passed through servers, reducing the risk of a security crack [19]. With the correct preventive controls, damages on the Cloud system will be minimized [21].

Corrective Controls- Corrective control is exactly what it says to its name, and are security issues that can be resolved quickly and efficiently after an attack, or an attempt on damage has been made, this real time security is important [19]. An example of a corrective control in place, may be a limitation on how much time is spent on your Cloud storage service, thus minimizing potential breaches. Compared to preventive controls, the correctives ones take control as an attack is taking place [21].

Detective Controls - Detective controls are the ‘Detectives’ of the Cloud controls. They detect any illegal users, who are working against the preventative and corrective controls to make sure there is minimal damage. Usually with detective controls, they can stop an attack before they even begin [19] by detecting the potential attack before it happens [21].

Furthermore, having the four storage cloud controls when accessing, or using a Cloud service can maintain its quality and storage [19]. The potential damage that can be limited due to the use of the controls, can prove extremely useful by the end of the online use to the cloud; the security of sensitive information can be completely secure if used properly. To make sure that the security of the cloud is secure, up to date and attack free, the security has to be in line with the standard security guidelines [21] with these security controls in place.

4. Cloud Users and Organisations

Many users today have an idea of the cloud being a glamourous security to their data and private documents, which delivers sufficient services based on their desires [22]. From a cloud user's view, a good cloud service will accommodate copious amounts of resources for its technicality. This means a user will always feel the need to be able to request more resources according to its need [22]. From an organisational perspective, the service is always providing elasticity, where the Cloud resources are adaptive to the business and user needs [22]. There are also several Cloud Security principles, which summarise the essential security principles when there is an evaluation towards the cloud services, and why they are important to an organization [23]. Some organisations wish to satisfy many of the security principles whilst many subsidize

5. Big Data Notion

Since the emergence of databases, businesses have immensely benefited from the data organisation capabilities that the databases offer. The history of relational databases traces back to 1974 when IBM initiated a project called IBM System R aiming at developing a database system for research purposes [24]. Though, the first commercial relational database was developed by Oracle in 1979 [25]. Relational databases are using tables (relations) to organise data records. Since then, there have been various techniques and architectures for relational database development. One of these initial established well-known techniques is the Cobb’s normalisation technique for redundancy reduction in the database [26]. Further extensions were added to Codd’s notion of normalisation. There were other novel techniques for developing object-oriented relational databases. Attaran & Hosseinian-Far proposed a hierarchical novel algorithm that derives the database from the relations of the system’s classes [27]. Big Data was initially defined by Magoulas in 2005 as “big data is when the size of the data becomes part of the problem” [28]. Goes associated big data with the four V’s attributes [29]. Volume is the first characteristic by which manipulation of large volumes of data is often considered within the realm of bi data science. The second characteristic is variety. The data types used for analytics in data science are varied and may belong to different industries and sectors. They are also often presented in different patterns and structures [30]. Most of this large volume of data are needed for real-time analytics and therefore the speed of transactions and data creation is often fast. Examples can be found in many sectors e.g. financial sector and banking in which transactions are to be updated in real time, or the stock market prices are to be analysed and informed rapidly [31]. The last V stands for Veracity by which the reliability of the gathered data is assessed. The big data veracity is very context dependent; for instance the data produced within the social networking context may contain irrelevant details including spams which would make the analytics task very challenging [32].

6. Fog Computing

Fog computing has emerged to address the need for low latency, location awareness, widespread geographical distribution, strong mobility, strong wireless access, strong presence of streaming and real time applications, and a support for the needed heterogeneity. All these characteristics of fog computing coupled with the advancement for wireless sensor networks (WSN) and Internet of Things (IoT) devices makes it suitable for the future of smart living. However there are research challenges remains active on security and privacy of cloud computing, fog computing, and IoT [9]. Our earlier work on cloud security has developed a generic framework known as Cloud Computing Adoption Framework [33]. However, privacy issues have not been addressed with respect to emerging IoT sensors, devices, cars, home appliances, drones and other applications that are expected to reach and use magnitude of location data as well as personal data.

The following section aims to forecast how these four emerging technologies i.e. Cloud Computing, Big Data Analytics, Fog Computing and Internet of Things, will work together for smart living.

7. Smart Living

The notion of smart living and cities is often described as a governmental initiative with a view to improve citizens' lives and living standards. Jimenez et al. believe that 'interoperability' between different organisations and departments is the main challenge to achieve smarter city perception [34]. There are number of enabling technologies which some are mentioned within this paper. There are numerous of applications to transform cities to smart cities; from education, communications, to infrastructure and energy, and beyond. Considering the application, an area of technology is required to enable the transformation process. The Internet of Things with its various technologies such as Wireless Sensor Networks (WSN's) is often considered to be an indispensable necessity. The overall idea is to reduce the energy consumption and costs, increase efficiency and enable faster data transfer from point A to B. Smart Grid is also considered as an essential enabling technologies which would reduce energy consumption intelligently. Narrow Band Power Line Communication (PLC) is an established technology which allows data transfer over the low-noise internal electricity wiring, whilst the Broadband PLC intends to transfer data over the city electricity grid. The main challenge to in implementation broadband PLC would be to overcome the noise [35]; nonetheless currently man electricity providers across in the UK and across the UK are moving towards smart metering.

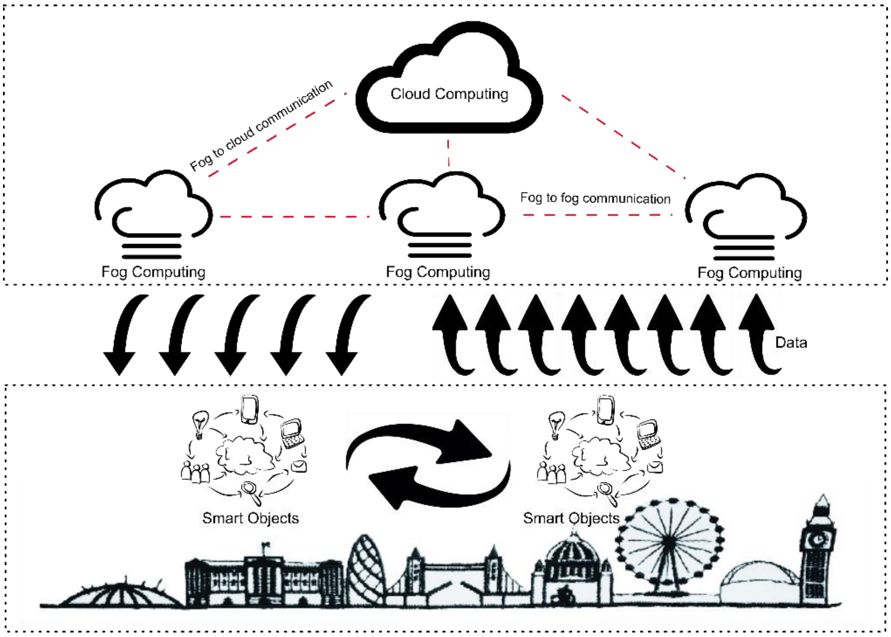


Figure 4: Cloud and Fog Computing, IoT and Data Generation (Own elaboration)

Real time monitoring and reduction of CO2 footprints is an essential step to ensuring the environmental friendliness of a smart city. A good example of this can be explained within the perspective of the London Plan. The London Plan authorised by the Greater London Authority (GLA) is a longitudinal development plan for the city of London, UK which outlines different policy principles for improving the quality of life and the city. The plan has undergone many modifications since its introduction in 2004. One of the sub policies of this spatial development plan is to reduce the CO2 footprint by 2050 [36]. Such a policy disposes the CO2 reduction through the use of solar panels, Combined Heat and Power (CHP) & Micro CHB, and insulation of the residential and industrial buildings (energy efficiency initiatives) as the applied approach to the policy [37]. These are accompanied by a set of executive targets; for instance, within the initial plan, the CO2 reduction is to be monitored every 5 years. This plan was followed the 'Smart London Plan' [38] in which the exploitation of Big data, IoT, Cloud Computing and in general digital technology could facilitate the initial longitudinal strategy. Big data technologies together with IoT would facilitate many of the monitoring and analysis tasks discussed within the initial proposal. The sensor networks could offer real time monitoring of the mart city's polluters, road traffic and any application in which the real-time monitoring is essential.

Cloud Computing would improve 'data storage', 'handling', and 'Caching' in the application of smart grid [39]. Rimal et al. have developed a novel resource management framework which utilises cloud computing for infrastructural networking [39]. Their research results assesses the use of cloud for broadband access traffic without affecting the performance in traditional architecture.

8. Conclusions

Cloud computing, big data analytics, fog computing & Internet of Things (IoT) are emerging and disruptive technologies that can enable smart living. This chapter aimed to outline an overview of these technologies and highlight the factors that would be necessary to consider before strategizing resources and applying the technologies within the context. Although the technology may seem not to be the bottleneck anymore for implementing digital systems in smart cities, nonetheless security, privacy and integrity are some of the notions that are alerting many policy makers and strategists before realising smart living through digital technologies.

References

[1] C. Babcock, Management Strategies for the Cloud Revolution, New York: McGraw Hill, 2010.

[2] R. Samani, J. Reavis and B. Honan, CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security, 2 ed., Syngress, 2015.

[3] L. Kleinrock, “A Vision of the Internet,” *ST Journal of Research,* vol. 2, pp. 4-5, 2005.

[4] S. K. Sood, “A combined approach to ensure data security in cloud computing,” *Journal of Network and Computer Applications,* vol. 35, no. 6, pp. 1831-1838, 2012.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing,” University of California at Berkeley, 2009.

[6] S. Dhar, “From outsourcing to Cloud computing: evolution of IT services,” *Management Research Review,* vol. 35, no. 8, pp. 664-675, 2012.

[7] V. Chang, “An overview, examples and impacts offered by Emerging Services and Analytics in Cloud Computing,” *International Journal of Information Management,* pp. 1-11, 2015.

[8] Cloud Security Aliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” December 2011. [Online]. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. [Accessed 2016].

[9] H. Jahankhani and A. Hosseinian-Far, “Challenges of Cloud Forensics,” in *Working Paper*, 2016.

[10] P. Mell and T. Grance, “The NIST Definition of Cloud,” US National Institute of Standards and Technology, Gaithersburg, MD, 2011.

[11] J. Ros, “Security in the Cloud: The threat of coexist with an unknown tenant on a public environment,” Royal Holloway,, London, 2012.

[12] Gartner, “Community Cloud,” 2016. [Online]. Available: http://www.gartner.com/it-glossary/community-cloud. [Accessed 2016].

[13] A. O. Joseph, J. W. Kathrine and R. Vijayan, “Cloud Security Mechanisms for Data Protection: A Survey,” *International Journal of Multimedia and Ubiquitous Engineering,* vol. 9, no. 9, pp. 81-90, 2014.

[14] Interoute, “What is a Hybrid Cloud?,” 2016. [Online]. Available: http://www.interoute.com/cloud-article/what-hybrid-cloud. [Accessed 2016].

[15] Y. Lu, X. Xu and J. Xu, “Development of a Hybrid Manufacturing Cloud,” *Journal of Manufacturing Systems,* vol. 33, no. 4, p. 551–566, 2014.

[16] H. Mouratidis, N. Argyropoulos and S. Shei, “Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach,” in *Domain-Specific Conceptual Modeling*, D. Karagiannis, H. C. Mayr and J. Mylopoulos, Eds., Springer, 2016, pp. 357-380.

[17] C. Kalloniatis, H. Mouratidis and S. Islam, “Evaluating cloud deployment scenarios based on security and privacy requirements,” *Requirements Engineering,* vol. 18, no. 4, p. 299–319, 2013.

[18] Cloud Council, “Security for Cloud Computing; Ten Steps to Ensure Success,” Cloud Standards Customer Council, 2015.

[19] CloudTweaks, “Cloud Storage Security Controls,” 2013. [Online]. Available: http://cloudtweaks.com/2013/03/cloud-storage-security-controls/. [Accessed 2016].

[20] D. Rawle, “Riding the Cloud Storm – Responding to Cloud Risks,” 2011. [Online]. Available:

http://www.bytes.co.uk/files/4514/0500/5660/david_rawle_-_cloud_security_challenges_presentation.pdf. [Accessed 2016].

[21] N. Chakraborty and R. S. Patel, “Security Challenges in Cloud Computing: A Comprehensive Study,” *International Journal of Computer Science Engineering and Technology(IJCSET) ,* vol. 4, no. 1, pp. 1-4, 2014.

[22] S. C. Park and S. Y. Ryoo, “An empirical investigation of end-users' switching toward cloud computing: A two factor theory perspective,” *Computers in Human Behavior,* vol. 29, no. 1, p. 160–170, 2013.

[23] CESG, “Summary of Cloud Security Principles,” 2014. [Online]. Available: https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles. [Accessed 2016].

[24] B. W. Wade, “IBM Relational Database Systems: The Early Years,” *IEEE Annals of the History of Computing,* vol. 34, no. 4, pp. 38-48, 2012.

[25] P. Ferreira, “The History of Oracle,” 2015. [Online]. Available: http://www.dba-oracle.com/t_history_oracle.htm. [Accessed 2016].

[26] E. F. Codd, “A relational model of data for large shared data banks,” *Communications of the ACM,* vol. 13, no. 6, pp. 377-387, 1970.

[27] H. Attaran and A. Hosseinian-Far, “A Novel Technique for Object Oriented Relational Database Design,” London, 2011.

[28] M. Loukides, “Big data is dead, long live big data: Thoughts heading to Strata,” 2013. [Online]. Available: http://radar.oreilly.com/2013/02/big-data-hype-and-longevity.html. [Accessed 2016].

[29] P. B. Goes, “Big data and IS research,” *MIS Quarterly,* vol. 38, no. 3, pp. 3-8, 2014.

[30] A. Abbasi, S. Sarker and R. H. Chiang, “Big Data Research in Information Systems: Toward an Inclusive Research Agenda,” *Journal of Association for Information Systems,* vol. 17, no. 2, pp. 2-31, 2016.

[31] U. Srivastava and S. Gopalkrishnan, “Impact of Big Data Analytics on Banking Sector: Learning for Indian Banks,” *Procedia Computer Science,* vol. 50, pp. 643-652, 2015.

[32] A. Abbasi and D. Adjeroh, “Social media analytics for smart health,” *IEEE Intelligent Systems,* vol. 29, no. 2, pp. 60-64, 2014.

[33] V. Chang and M. Ramachandran, “Towards achieving Cloud Data Security with the Cloud Computing Adoption Framework,” *IEEE Transaction on Service Computing,* vol. 9, no. 1, pp. 138-151, 2016.

[34] C. E. Jimenez, A. Solanas and F. Falcone, “E-Government Interoperability: Linking Open and Smart Government,” *IEEE Computer Society,* vol. 47, no. 10, pp. 22-24, 2014.

[35] A. Hosseinpournajarkolaei, H. Jahankhani and A. Hosseinian-Far, “Vulnerability considerations for power line communication's supervisory control and data acquisition,” *International Journal of Electronic Security and Digital Forensics,* vol. 6, no. 2, pp. 104-114, 2014.

[36] A. Hosseinian-Far, E. Pimenidis and H. Jahankhani, “Financial Assessment of London Plan Policy 4A. 2 by Probabilistic Inference and Influence Diagrams,” in *Artificial Intelligence Applications and Innovations*, vol. 364, Berlin Heidelberg, Springer , 2011, pp. 51-60.

[37] A. Hosseinian-Far, H. Jahankhani and E. Pimenidis, “Using Probabilistic Networks for the London Plan Knowledge Representation,” in *10th IEEE International Conference On Cybernetic Intelligent Systems*, London, 2011.

[38] London Mayor's Office, “Smart London Plan,” London.gov.uk, London, 2013.

[39] B. P. Rimal, D. P. Van and M. Maier, “Mobile-Edge Computing vs. Centralized Cloud Computing in Fiber-Wireless Access Networks,” in

2016 IEEE Infocom 5G & Beyond Workshop, San Francisco, USA, 2016.