Cloud Computing Regulations and Readiness: Comparison Study (United Kingdom, Germany and Hungary)

Elias R. Jreissat

Faculty of Informatics, Department of Applied Mathematics and Probability Theory, University of Debrecen, 4028 Debrecen, Hungary

E-Mail: elias.jreissat@inf.unideb.hu

ABSTRACT

This paper elucidates the general concept of Cloud computing and puts forward the key points that should be taken into consideration while applying Cloud service's models such as (IaaS), (PaaS) and (SaaS), regardless which type is used, whether it is Public, private, hybrid or even community cloud's type. in addition, a comparison between three European countries was also conducted, proposing the most well-known regulations issued by several specialized European authorities. Furthermore, an assessment has been carried out, genuinely based on the BSA Global Cloud computing Scorecard 2016 combined with the results of a survey filled out recently by some specialists from the Hungarian side. afterwards, some formulas have been suggested based on this assessment, and showed that the UK is a leading country concerning the readiness for cloud services. Germany, too, compete strongly in some major fields such as Data Privacy and Promoting Free Trade. conversely, Hungary has surpassed both of them in the Data Privacy field, and outranking Germany in the fields of Security and Cybercrime.

Keywords: Cloud computing · Infrastructure as a service (IaaS) · Platform as a service (PaaS) · Software as a Service (SaaS) · Public cloud · Private cloud · Hybrid cloud

INTRODUCTION

Nowadays, we are witnessing a dramatic era of rapid developments in the domain of IT solutions, intended to facilitate work processes and procedures. However, one of the most valued new fashion trends, which is leading the market lately and is considered as an outsource service aligned with the IT department in most institutions, is Cloud Computing. "Cloud computing is known as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems, too intensive for any stand-alone machine" [1]. It has now become commonplace for many institutions to use the effectuation of Cloud Computing services. This has happened because of the positive effects such services have on the different levels of any given institution, especially with regard to facilitating business process and simplifying information storage methods, saving time and efforts, and enabling the organization to reduce expenses that are allotted to cover the IT department needs. Cloud is mainly divided into the following three types: public, hybrid, and private cloud [2]. This study illustrates not only the general considerations that should be taken when applying cloud computing, but also compares such regulations and readiness in three European countries namely; UK, Germany and Hungary. The rationale behind specifically selecting these three countries to carry out the comparison is, first, that Germany and UK are considered as two of the top leaders for several areas (mainly economics and regulations) in Europe. Second, Germany and UK were ranked the 3rd and the 9th countries in the Global Cloud Computing Scorecard, respectively. Such scorecard was classified by the leading advocate for the global software industry and considered the first of its kind to rank 24 countries worldwide, account for 80 percent of the global information & communications technology market and assess seven sets of indicators; data privacy, cyber security, cybercrime, intellectual property, technology interoperability and legal harmonization, free trade, and IT infrastructure[3]. Moreover, for public sector use of ICT (Information and Communications Technology), the UK's G-Cloud Strategy is the most fully elaborated cloud policy in Europe that adopts a "public cloud first" approach for public procurement[4]. Germany is considered as a great location for cloud computing services compared to others worldwide, and its restrictive laws threaten to undermine the spirit of those same laws, for instance, geographic restrictions should be set on data that are neither needed to protect certain classes of data nor supported by law. Also, practices in Germany could weaken its own potential for any success in the cloud[3]. In Hungary, clouding is one of the emerging and growing areas that attract the concern of many authorities nowadays especially the national central bank (MNB) which focuses on the applicability of Cloud Computing in the financial sector, measuring the risks and finding ways to mitigate them through their regulations. The comparative study carried out in this paper answered the following questions:

1. What is cloud-computing and how would it benefit any institution?

2. Is cloud-computing service able to operate freely out of laws that are discriminated based on the nationality of vendor, developer, or service provider?
3. What kind of policies regulates the process of data transmission in different service levels?
4. What kind of assessments should be prepared in case of willing to apply outsource cloud- computing and what appropriate processes should be adopted?
5. How does the effectiveness of access to data and premises in Outsourced services solutions affect the role of audit?
6. How should institutions manage the process of change and how essential is the existence of a periodically reviewed business continuity plan is?
7. Are there any precise points that should be included in a termination agreement and how does exit plans affect the work procedures?
8. What precautions should be taken in case of outsourcing cloud system provider failure and what should be done in case of a virtual or physical security breach?
9. Do the financial institutions require special regulations for applying cloud systems? In addition, are there any particular authorities responsible for such legalizations?
10. Does applying cloud-computing service require the compliance to the international standard & regulations or just compliance of the regional local policies and set of laws?

RELATED WORK

There are several definitions of cloud computing clarified by special authorities located in the three countries under comparison: Firstly from Financial Conduct Authority (FCA) (United Kingdom) *"Clouding could be defined as encompassing a range of IT services provided in various formats over the internet, including private, public or hybrid cloud, as well as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS); Cloud services are constantly evolving"* [5]. Secondly from Hungarian National Bank (MNB) (Hungary) *"The computing cloud is a solution that enables network access to shared, configurable computing resources (networks, servers, storage devices, applications and services) on demand, which can be allocated quickly and close the usage thereof, with minimal management efforts or interaction from the service provider, who can serve several customers and allocates the various physical and virtual resources dynamically in line with user needs, both ways this service could be used on demand even on self-serve basis, also could be accessed (through the Internet or a private network), and it has the feature of Fast reaction to changing capacity needs"* [6] and lastly from Federal Office for Information Security (Germany) *"Cloud is understood as offering, using and billing IT services dynamically adapted to the requirements via a network. Here, these services are only offered and used by means of defined technical interfaces and logs. The range of the services offered within the cloud computing framework covers the entire spectrum of information technology and, among other things, includes infrastructure (e.g. computing power, storage space), platforms and software, service could be obtained from public, private or hybrid cloud"* [7]. In General, infrastructures, platforms or services that run on a distributed network using virtual resources and accessed by several Internet protocols and network standards are identified as Cloud-Computing[8]. Cloud turns alike services, applications, and technology applied on the internet to self-service utility. Two main concepts worth to be clarified as follows:

- Virtualization: systems are virtualized by pooling and sharing resources in cloud computing. Centralized infrastructure can provide systems and storage, assessment of costs are on the metered basis, scaling resources by agility, and enabling multi-tenancy concept.
- Abstraction: Applications run on physical systems that aren't specified. Administration of systems is outsourced to others, and access by users is ubiquitous. Cloud computing abstracts the details of system implementation from users and developers, and data are stored in locations that are unknown[9]. The main service models in cloud computing based on the definition of National Institute of Standards and Technology (NIST) are:
- Infrastructure as a Service, IaaS: the service provides gives virtual hardware, and the user installs and operates all software on it.
- Platform as a Service, PaaS: the service provider provides virtual hardware and platform software (usually operating system, database software and web server), and the user installs and operates its own business applications.
- Software as a Service, SaaS: the service provider provides a business solution operating on the virtual hardware and platform software; this is configured and partly operated by the user (e.g. user access management)[10-12].

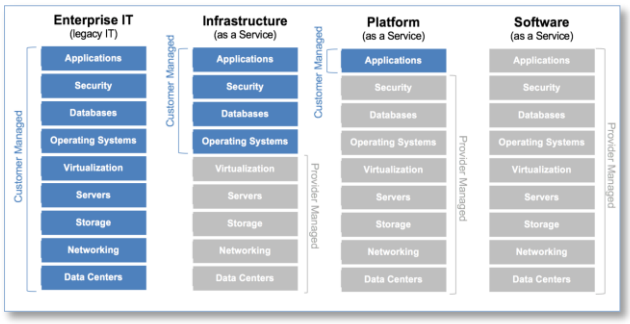

Figure 1: Cloud Computing Service Models [10, 11].

As shown in figure 1 above, The idea of (IaaS) model can be explained as renting a vehicle in which the customer is not responsible for its repair since it is the owner's responsibility and he is only responsible for supplying the vehicle with fuel thus he can go pretty much wherever he wants to, therefore in the IaaS model, the customer just needs to do some system settings, maintains software, etc and he is free to manage it the way he likes to. On the other hand, (PaaS) model is a little bit different, actually almost like getting a taxi; the customer can choose where to go and which way to take but keeping the taxi running and figuring out the details

is up to the driver. Finally (SaaS) Model is most often like using public transportation, of course, it is cheaper, but someone else takes care of pretty much everything; the customer just use it, and most of the time he just doesn't get as close as he wants (much less customizability). Anyway, special requirements always apply to different kinds of institutions and perhaps determined by the function's type which is outsourced. The function being outsourced or not, whether it is material outsourcing or Important operational functions is something classified as important or critical[13, 14]. Specific terms in respect of outsourcing are defined in regulations as follows:

- Critical or important – an operational function is being defined as critical or important if it has failures or defect in its performance resulting in weakening its compliance with obligations, regulations and terms either under its own authorization or any other regulatory systems, whether it affects the firm's financial performance, or the continuity of the firm's relevant services and activities (Senior Management Arrangements, Systems and Controls (SYSC 8.1.4R)) [5].
- Material outsourcing – defined as outsourcing of important services in which any fault or deficiency of such service can cause doubts of the firm's continuing satisfaction of the threshold conditions or compliance with the Principles for Businesses (PRIN) [13, 15].
- Important operational functions – As what is listed under the Electronic Money Regulations 2011 and the Payment Services Regulations 2009, an operational function is important if a defect or failure in its performance would materially impair:
  i. The authorized institutions compliance with the regulations and any requirement of its authorization;
  ii. The authorized institution financial performance;
  iii. The authorized institution soundness or continuity [13, 15].

Recent Researches on protected cloud computing is still focusing on the security level of cloud storage with less consideration of the security level of outsourced computation. Furthermore, it was proved by the meltdown of Gmail systems that the cloud computing servers can be considered as a single point of failure as assured by some centralized architectures. On the other hand, cloud computing servers may act as they are performing the required computations in order to save the resources of computation [16]. Cloud servers may behave in a cheating way while performing unreliable computation operations in a hidden way in case of complex failures or external attacks but it may deliver useless results if not detected [17]. In case of any detected problem and for accountability purposes, appropriate mechanisms of secure computation should determine the responsible party who's in charge for such problems whether the user or the cloud server, keeping into consideration that, servers naturally suspect problems with the customer's software [18]. Using Cloud computing may provide more pliability to the services that any firm might receive, allowing for more innovation and bringing more benefits to the firms, their customers, and the market. However; it can create new risks affecting the firm's data security or control level as well as a slighter control for customers using the Cloud over their providers, those new identified risks need to be well recognized, observed and alleviated [19]. On the other hand, Cloud Auditing or verification costs might not be affordable by the Cloud users due to the constraints in communication and computation resources and to reduce such expensive costs, trusted auditors can be assigned to lead the cloud audit process. However; public auditing receives less attention although they have the ability to secure storage in cloud [20, 21]. On the other hand, distributed systems rely widely on the concept of secure remote computation [22]. Secure computing auditing in cloud can be conducted through a double-check of results initially computed by cloud providers and auditors separately and then through comparing their both outcomes. However, this might lead to a loss of Input/output and computation resources, noting that the overall success of the cloud computing might be affected by data transferring bottlenecks which is classified as one of the top ten obstacles averting its success [23]. Venters and Whitley (2012) elucidate the main businesses' need from cloud computing especially in terms of equality between "technical services that are alike as well abstracted" and "technical services that abstract away unnecessary complexity", as well as creativity, efficiency, simplicity and scalability. The distinctive nature of cloud computing helps to create business innovation and derive creativity since cloud providers and cloud offerings are becoming more abundant and mature day after day [24].
Moreover, Security of cloud is one of the vital issues in such areas, but Regular grid computing introduces CBS (Commitment-Based Sampling) technique without being concerned about privacy issues. Meanwhile, cloud computing security and privacy are considered to be the main issues as most researchers divided them into cloud computation security and cloud storage security [25]. PDP model (Provable Data Possession) clarifies that stored data at any unreliable server should be verified by clients assuring that the server possessed the original data without retrieving it. However, in such cases similar tags that are based on RSA for auditing outsourced data were used without considering a dynamic data storage [26]. Nevertheless, a bunch of cloud computing risks for providers, their partners, and their customers has occurred because of this complex environment of cloud-based business services innovation. From the customer's perspective it could be a risky decision to shift from on-premise to the cloud. Furthermore, the shifting from premises to the cloud strongly impacts intra-organizational interfaces[27]. Key risks of cloud for organizations relay to identity software isolation, compliance, management, security responses and governance [19/28]. Consequently, the impact of cloud computing goes away beyond the IT and affects the whole of the business[29]. Mainly, the service provider's responsibility is to manage the resources to accomplish end users' requests. They utilize scheduling algorithms to plan the incoming requests (tasks) and to

professionally manage the resources of computing. Managing resources and scheduling tasks allow providers to exploit utilization of resources and maximize revenues. In live out, scheduling and allocation of resources are essential barriers in terms of cloud computing resources performance [30]. Damsgaard et al.[31] suggested that managers should consider how cloud services can convert the entire business instead of thinking about the capability of cloud to affect and change the IT functions[31]. The involved decisions may potentially have terrible consequences. Furthermore, Business leaders should proactively develop an overall strategy and timeline regarding which applications they can move to the cloud [32]. Oppositely, it is the responsibility of the customer to identify the risks in all phases of the cloud service lifecycle, and to implement proportionate protection measures, others see that the cloud provider is responsible for the design, description, implementation and effective operations of organizational and operational measures (controls) with which the requirements are implemented at the cloud provider side[33]. What gives any business an elastic budgetary framework so they can outsource the needs of technology in their firm while focusing other resources on enriching business capabilities is the "pay-as-you-go model"[34]. Much like, in large and small-to-medium enterprises (SMEs), the essential impulsion behind cloud computing was mainly the need to outsource supporting tasks and accent on core business results. Therefore, the attention from managing technology assets was shifted to consider the customer value in using technology services[27, 35]. Haibach [36] assured that cloud computing services exceeded the territorial borders, and providers nowadays are offering their services worldwide targeting a larger market through global intermediaries and external subcontractors, therefore, he concentrated on the contracting practices and conditions regarding cloud computing based on the EU private international law rules and clarified that such international laws are protecting customers, considering the jurisdiction and other applicable clauses of law , assuring that access to the EU courts for consumers would ensure the mandatory provisions enforcement of EU international or other national law [36]. The creativity inspired by cloud has arisen from an ecosystem that lowers the barriers to innovation by allowing cloud providers to give organizations an access to a rich pool of instruments to design innovative solutions for their customers by forcing open source computing resources, with third-party application providers accompanying the cloud platform and offering a wide-ranging set of tools and building blocks for architecting desirable end-to-end business outcomes [32]. At an extremely vital period Cloud computing new standards and regulations have been raised in a time when companies needed solutions to reduce the load of administration and cost of operations, it was published by IEC and ISO in 2014 (ISO/IEC 27018) titled by "Information technology security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors", helping Cloud services' providers to meet the terms of their contracts legal aspects when they process their own personal data, by acting as data processors, creating cloud control mechanism and other controls for clients, at last, the communication 'Unleashing the Potential of Cloud Computing in Europe' was released in 2012 by the European commission to accelerate cloud absorption in Europe countries [37]. From a business point of view there is a developing body of knowledge face to face with cloud computing which goes beyond the primary focus on the adoption and implementation of technology. The provider of Business services based on cloud, as well as their business partners and other stakeholders are obviously in dreadful need of models that are able to help them specify the challenges' host that they face during the innovation process of services[38]. Finally Zwattendorfer et al.[39] examined 8countries in the European Union, and compared how these countries used cloud computing in e-Government. The study resulted, by a clarification that deployment of cloud computing model so-called G-Cloud (Governmental Cloud), or community or private cloud particularly designed for the use of national governmental. However no favoured cloud service model has emerged, hence all the standard models of cloud service as (Platform, Software and Infrastructure as a Service) are adopted by most countries. Also, Cloud computing had been anchored in half of the tested European countries in one of their national strategies of ICT [39].

COMPARISON STUDY

All legal information mentioned below was mainly collected based on regulations legislate by some main authorized parties in three European Countries.

a) **United Kingdom**: Financial conduct Authority (FCA), Prudential Regulation Authority (PRA), Data Act Protection (DAP), UK Government regulations, Bank Of England.
b) **Hungary**: Hungarian National Bank (MNB), Hungarian Financial Supervisory Authority (HFSA), National Authority for Data Protection & Freedom of Information in Hungary.
c) **Germany**: Federal Office for Information Security (BSI)

Following are the most six important sections that have been considered in the comparison study due to their essential influence on cloud computing services implementation.

Regulatory Considerations & International Standards

The British regulatory considerations is that initially any institution should have a documented business case to support the decision of outsourcing , considering any relevant regulatory obligations as well as probable Risks and make sure that the outsource agreement will not worsen the Firm's operational risk , taking into consideration the jurisdiction key point which is so vital for regulation determination and in case the service provider is located out of UK then the contract also should guarantee auditor's & regulator's effective access to data and business premises, on the other hand adherence of the provider to the international standards is required, taking into account the importance of external assurance since it might be more relevant regarding

well understood standards and stabilized assessed services in data centres [5, 8, 15, 40]. On the other hand Hungarian authorities stress the need of regulatory compliance before using the cloud service after assessing the detailed tasks in the decision drafting phase, and ensure the necessity of essential controls and monitoring capabilities by the provider , furthermore it forces compliance to the regulations of the "Act L of 2103" electronic information security if systems are identified as an entity of key importance in the financial sector, apart from this they concentrate on monitoring the changes in the regulations of the EU as well as the Hungarian National Bank (MNB) regulations and international EU data privacy provisions and practices[6, 8, 15, 41, 42]. What is an addition in Germany is that responsible parties should assure a high degree of trust in the cloud service provider before the implementation phase. They consider the cloud computing compliance controls catalogue (C5) as the baseline to be an aid for the customer, intended to provide a better overview for a higher level of security and avoid redundant audits, in addition to some international standards that should be taken into consideration such as (ISO/IEC 27001:2013; CSA3; AICPA4; IDW6; ERS FAIT 5; BSI IT)[7, 15].

Risk Management

Assessing risks is one of the serious aspects that firms should focus on, therefore, some parties in UK ensure that firms should have a documented risk identification, assessment, and mitigation plan for such identified risks especially jurisdictional risk-previously mentioned- for its significant impact on business procedures. Keeping in mind the firm's responsibilities in assessing, managing and monitoring operational and concentration risks and business recovery in case of failure from outsource provider or a notification of breach[5, 8, 15, 40].Other parties in Hungary strengthen the concept of the I.T risk analysis by operating controllers set either by the institution or by the service provider to ensure conformity of the requirements in cloud service security principles and phases of service's lifecycle as agreed upon in the signed contract whereas The firms shall manage risks causing regulatory noncompliance with risk mitigation actions and define the level of required assurance according to the risk level of the areas involved[6, 8, 15, 41, 42]. However Germans do have a different point of view, since some of the knowledgeable authorities see that policies and instructions for the general procedure applicable of risk identification, analysis, assessment and handling including IT risks are documented, communicated and provided according to (SA-01), This procedure is at least done once a year taking into account internal and external changes and influencing factors. Risk management policy in any firm must include top management parameters' for the risk appetite and risk tolerances of the cloud provider in addition to the acceptance of the identified risks, documentation, assessment and mitigating safeguards[7, 15].

Data Security And Data Protection

Experts in UK believe that a security assessment and a Data residency policy with the provider should be carried out by a firm, besides providers' data loss & breach notification processes that should be aligned with the firm's risk appetite and legal or regulatory obligations, but In case of using public clouding then data segregation and data sensitivity should be considered, keeping into account the appropriate steps to mitigate security risks and to keep an acceptable overall security exposure in the firm, in general institutions should comply at least with the main principles of the DPA (Data Protection Authority) [5, 8, 15, 40]. On the other hand authorized parties in Hungary assure that the institution should identify and applies security classification to the data that is planned to be outsourced to the cloud service provider in line with the legal regulations and its own data protection rules as specified in "NAIH" the Hungarian national authority for data protection and freedom of information, after all a definition of data security requirements should be adopted also stored data should be protected from unauthorized access and modification as well as several types of data transmission such as (transmissions between the institution and the cloud, between the resources in the cloud and between the cloud and other external service providers).keeping into account that security incidents and their resolution should be declared, and the provider should support any regulated fraud's investigation, moreover institutions should support protection against malicious codes, including the installation, regular update and central monitoring of security tools, as well as regular antivirus checking of the network and devices, however the institution supposed to obtains assurance that the cloud service provider adheres to the relevant data protection rules and legal regulations as mentioned previously and identifies the differences between the data protection requirements relevant to the institution and the cloud service provider's data protection commitments, practices and data reporting obligations relying on the contractual conditions, and last of all ensures the safe handling and processing of personal, banking and insurance data, as well as data classified as secret by other sectorial laws, in compliance with the data protection regulation[6, 8, 15, 41, 42]. Conversely Germans reassure that the security of cloud services is an ongoing task so data of the cloud customer shall only be processed, stored and backed up outside the contractually agreed locations only with the prior express written consent of the cloud customer and cloud provider must use secure network protocols for the import and export of information as well as for the management of the service in order to ensure the integrity, confidentiality and availability of the transported data moreover there are requirements for the protection of personal data according to BDSG (German Federal Data Protection Act) or EU Data Protection Directive, boils down to the following: Legal permission /consent, Direct collection, Data minimization, Purpose limitation, Transparency, etc[7, 15].

Effective Access To Data & Business Premises

Regulated firms should require effective access for the auditors, regulators and relevant competent authorities, to data which is related to its outsourced activities offered by service providers as what UK expert parties advise for, and they see that notification requirements on accessing data should be reasonable without restrictions on auditors and regulator's access since they must treat any information disclosed in accordance with the confidentiality obligation

set out in (FSMA), at the same time Contracts should enable them to contact service provider directly in case firm cannot disclose data for any reason also in some cases contracts must allow business premises' access, which are relevant for the exercise of effective oversight beside it is preferable to provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation, at times scope of visit could be limited only to the services that are used by the firm's group[5, 8, 15, 40]. In the same way Hungarian experts assure that data stored in the cloud should be protected from unauthorized access and modification, and it's availability is ensured since sufficient logical data access controls is considered as one of the data security requirements within its scope of authority, so the institution should establish a documented and approved user and access rights management procedure, which should be at least at an equal level with the procedure used for local systems and it should cover the processes for requesting, approval, setting up access rights, regular review and revocation keeping into consideration that privileged users which are identified by multi-factor authentication as well as comprehensive and up-to-date records of authorized users and their access rights, should be documented, also all the above should be monitored regularly. In the same way the institution should obtains assurance that its resources located in the cloud are protected against unauthorized physical or logical access, damage and theft, also that the cloud service provider's data centres are protected much as Physical access and environmental controls of physical resources, as well as the necessity of assuring the Management of cryptographic keys[6, 8, 15, 41, 42]. While Germans experts concentrate on the necessitate to document the role and rights concept based on the business and security requirements of the cloud provider as well as the policy for the management of system and data access authorizations which are responsible of rolling the granting and changing processes of data access authorizations for users under the responsibility of the cloud provider, at the same level the perimeter of premises or buildings which lodge sensitive or critical information, information systems or other network infrastructure are protected in a physically solid manner and by means of appropriate security safeguards much as Structural, technical and organizational safeguards to protect sites from unwanted physical access or against natural threats such as fire, water, earthquakes, explosions, civil disturbances [7, 15]

Change Management And Continuity Plan

In view of the fact that risks can be introduced when changes are made to processes and procedures, UK expert authorities advice that firms should have a comprehensive change management process, establishing what provision has been made for making future changes to technology service provision and how the testing of changes will be carried out, on the other hand Firm should have arrangements to ensure that it can continue to function and meet its regulatory obligations if outsourced services are interrupted, considering Likelihood and Impact of an unexpected disruption not forgetting the documentation of firms' strategy, including recovery from an event, plans for communicating and regularly testing[5, 8, 15, 40]. However Hungarian authorities recommend institutions to obtain assurance regularly of the cloud service provider's full compliance with data security and protection requirements – at least annually, or after significant changes in the relevant business process, service, configuration or legal environment keeping into consideration that some institutions also might rely on independent third parties' audits or certifications for obtaining assurance[6, 8, 15, 41, 42]. Analogous to German expert parties who advocate to the need of comply with the security targets in case of new developments and procurement of information systems as well as changes, then all changes should be categorized, prioritized, subjected to tests during the development phase on the basis of a risk assessment in order to obtain an appropriate authorization prior to making the change available to the production environment, furthermore configuration objects which might be affected by the change should be assessed with regard to potential impacts not forgetting that Emergency changes also should be classified by the change manager who creates the change documentation before applying the change to the production environment, but the main value conclude in top management who specified as the process owner of the business continuity and contingency management and bears the responsibility for the establishment of processes in the company as well as the compliance with the policies also they must ensure that adequate resources are made available for an effective process, last of all and based on the business impact analysis, a uniform framework for planning the business continuity and business plan is introduced, documented and applied in order to ensure that all plans are consistent [7, 15].

Exit Plan

In UK, experts' clarify that firms need to ensure the capability of exiting outsourcing plans without undue disruption to their provision of services or their compliance with regulatory regime so firms should have understood, documented and fully tested exit plans and termination agreement to maintain business continuity in case of transition to an alternative service provider, and consider obligations to ensure outsourcing provider cooperate with the systems on exit, above all to monitor concentration risk and consider what actions should be taken in case of outsource provider failure[5, 8, 15, 40]. Much like previously Hungarians suggest that institutions should prepares an exit strategy and an action plan in order to lower the risks also they should stipulates such service conditions that allow the exit from the cloud without Difficulty especially in the process of providing the stored data in a format that can be interpreted and used irrespectively of the cloud service; Ensures and tests the operability of the impacted business processes in case the cloud service is discontinued with a risk proportionate method and frequency[6, 8, 15, 41, 42]. Finally Germans parties advise that, to maintain business continuity the institutions should simply carry out the following several steps that should be defined in the exit strategy and action plan during the exit process:

- Installation of migration tools;
- Testing the downloading of the data in a test environment;

- Downloading the data in the production environment, and taking back the service based on the scripts;
- Validating based on the acceptance criteria; verifying the correctness of the data taken back; and closing the migration;
- Follow-up for fixing errors after migration;
- After the successful exit from the cloud, deleting the data at the service provider, including both live, backup and archiving environments according to the contractual conditions; the service provider shall provide assurance (declaration) of deleting the data.
- Terminating the unnecessary IT and communication connections with the service provider [7, 15].

MATRIX: BSA GLOBAL CLOUD COMPUTING SCORECARD (2016)

The below table shows the responds of United kingdom & Germany regarding several inquiries, collected from the latest BSA survey study (2016) and merged with the Hungarian respond which had been also collected from the Hungarian national bank authority through having several meetings with the authorized people.

As noticed in the table below, in the first two sections clarifies a huge approximation between the three countries at various levels, whether in E.U data protection, adjustment with the Asian-Pacific Economic Cooperation, or even electronic signature regulations and more. On the other hand we can notice the differences occur in the section of registration requirement of data controllers whereas it is not free at all in UK, in addition the difference occurs in the third and fourth sections which concludes in cybercrime Budapest convention consistency, cloud computing service laws and data transmission laws and policies , criminal sanctions of copyrights on internet, and finally the ability of cloud computing services to operate free from laws and policies which is also considered as a very critical point and should be taken into consideration and dealt with in a cautious and serious way.

Table 1: Global Cloud Computing Scorecard (2016)

No.	Question	UK	Germany	Hungary
Data Privacy				
1	Are there laws or regulations governing the collection, use, or other processing of personal information?	Yes	Yes	Yes
2	Is the privacy law compatible with the Privacy Principles in the EU Data Protection Directive?	Yes	Yes	Yes
3	Is the privacy law compatible with the Privacy Principles in the APEC Privacy Framework?	Yes	Yes	Yes
4	Is an independent private right of action available for breaches of data privacy?	Available	Available	Available
5	Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	Sectorial regulator	National regulator	National regulator
6	Are data controllers free from registration requirements?	Partial	Not Free	Not Free
7	Are cross-border transfers free from registration requirements?	Yes	Yes	Yes
8	Is there a breach notification law?	Partial	Partial	Partial
Security				
9	Is there a law or regulation that gives electronic signatures clear legal weight?	Yes	Yes	Yes
10	Are ISPs and content service providers free from mandatory filtering or censoring?	Yes	Partial	Yes
11	Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	Limited coverage in legislation	Limited coverage in legislation
Cybercrime				
12	Are cybercrime laws in place?	Yes	Yes	Yes
13	What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers or other service providers?	Unlimited access	Access with a warrant	Not stated
14	Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	Yes	Partial	Yes
Intellectual Property Rights				
15	Is the country a member of the TRIPS Agreement?	Yes	Yes	Yes
16	Have IP laws been enacted to implement TRIPS?	Yes	Yes	Yes
17	Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	Yes	Partial	Partial
18	Are there laws governing ISP liability for content that infringes copyright?	Yes	Yes	Yes
19	Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	Compreh-ensive protection	Compreh-ensive protection	Limited protection
Support for Industry-Led Standards & International Harmonization of Rules				
20	Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	Yes	Yes	Yes
21	Is there a regulatory body responsible for standards development for the country?	Yes	Yes	Yes
22	Are international standards favored over domestic standards?	Yes	Yes	Partial
23	Does the government participate in international standards setting process?	Yes	Yes	Yes
Promoting Free Trade				
24	Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	No	Yes	Yes
25	Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	No	Partial	Partial
26	Are "cloud computing" services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	Yes	Yes	Yes
IT Readiness, Broadband Deployment				

27	Are there laws or policies that regulate the establishment of different service levels for data transmission based on the nature of data transmitted?	Regulation under consideration by government and extensive public debate	Regulation under consideration by government and extensive public debate	No

DATA ANALYSIS METHODOLOGY

The content of the above semi questionnaire (Table 1) was adopted by the BSA 2016 Annual Global Cloud Computing Scorecard; some major questions were collected to investigate the extent of aptitude, disposition, and inclination in those three EU countries for implementing and hosting Cloud computing services. Questions had been weighted due to its importance and impact on cloud services, it was divided into seven main fields, each field contains bunch of questions having different weights and totalled by (100%) per section, as well as each field has its own different weight with a total of (100%) as the following: (Data Privacy "10%", Security "10%", Cybercrime "10%", Intellectual Property Rights "20%", Support for industry-led standards "10%", Promoting Free Trade "10%", and IT Readiness "30%".

Formula one:

Assume that Qw = *Question weight,* $I\mu 1$ = *Importance,* $I\mu 2$ = *Impact,* Tn = *Total number of questions.*

Then, Equation (1) $$Qw = \frac{I\mu 1 \times I\mu 2}{Tn}$$

Formula Two:

Assume that $A\Gamma$ = *Answer Ratio,* $L\delta\Delta$ = *Likert scale answers, (Yes = "100", Partial = "50", No= "0").*

Then Equation (2) $$A\Gamma = \frac{Qw \times L\delta\Delta}{100}$$

Finally the total ratio for each country per section equal to the SUM of the answers' values in that section. Equation (3) (See figures 2-8 below).

The following "7" listed figures (2-8) which clarify the results after rating all of the previous questions in the above questionnaire (Table1) based on BSA 2016 scoring plus the MNB replies, followed by applying the previous formulas to get the following results:

Question Num	United Kingdom	Germany	Hungary	
1				%
2				%
3	30	30	30	%
4				%
5	12.5	25	25	%
6	10	0	0	%
7	15	15	15	%
8	5	5	5	%
Total	72.5%	75%	75%	

DATA PRIVACY

Figure 2: Data privacy ratio

Question Num	United Kingdom	Germany	Hungary	
9	34	34	34	%
10	33	16.5	33	%
11	33	33	33	%
Total	100%	85.5%	100%	

SECURITY

Figure 3: Security ratio

Question Num	United Kingdom	Germany	Hungary	
12	54	54	54	%
13	12	6	0	%
14	34	17	34	%
Total	100%	77%	88%	

CYBERCRIME

Figure 4: Cybercrime ratio

Question Num	United Kingdom	Germany	Hungary	
15	18	18	18	%
16	18	18	18	%
17	18	9	9	%
18	10	10	10	%
19	36	36	16	%
Total	100%	91%	73%	

INTELLECTUAL PROPERTY RIGHTS

Figure 5: Intellectual property rights ratio

General Indicators	Germany	United Kingdom	Hungary
Population (millions) (2014)	83	63	9.8
Population Density (people per square km) (2014)	232	267	106
Per Capita GDP (US$ 2014)	47.627	45.603	28,565
IT Service Exports (2014) (billions of US$)	108.1	120.5	7.3
IT Readiness Indicators			
Internet Users (millions) (2014)	69	57	7.770
International Connectivity Score (2014) (Score is out of 10)	5.42	5.90	4.2
International Internet Bandwidth (2014) (bits per second per Internet user)	145.990	429.830	154,765
Fixed Broadband Subscriptions (millions) (2014)	29	23	2.8
Active Mobile Broadband Subscriptions per 100 inhabitants (2014)	64	89	41
Number of Active Mobile Broadband Subscriptions (millions) (2014)	53	56	4
Indicators values were collected from the BSA annual report merged with the values collected from the authorized parties in Hungary such as (MNB) the National Bank of Hungary			

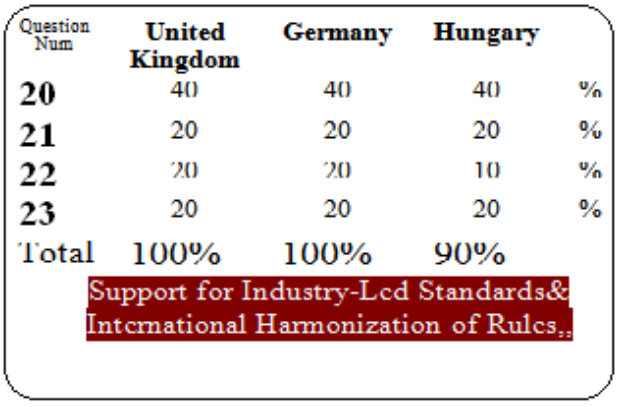

Figure 6: Support for industry-led standards & international harmonization of rules ratio

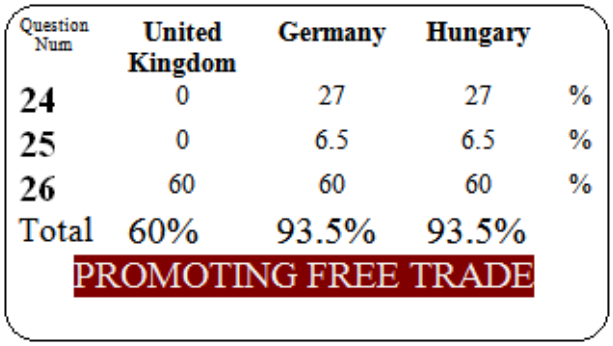

Figure 7: Promoting free trade ratio

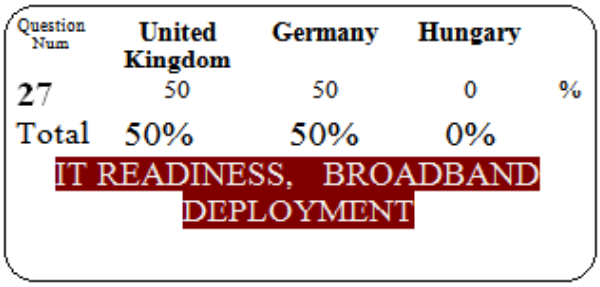

Figure 8: IT readiness, broadband deployment ratio

Table 2: Important Indicators, IT Readiness (Germany, United Kingdom, Hungary)[43-45].

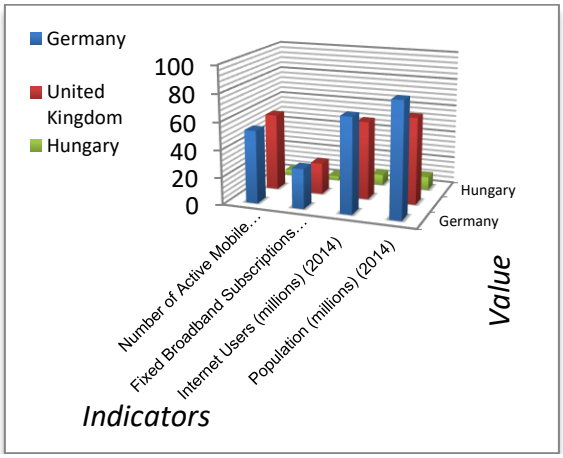

Figure 9: Population Indicator Internet versus

Figure 9 above, based on (Table 2) shows the population in the three countries mentioned earlier, compared with the number of internet users, where we note that the largest census of the population are considered to be users of internet services of all types, divided into two main parts, the first section, which represents almost one third of the total number of internet users considered as fixed broadband subscribers, while the largest part of nearly two-thirds of the total number of internet users is considered as a mobile internet users of all types whether on mobiles or other devices.

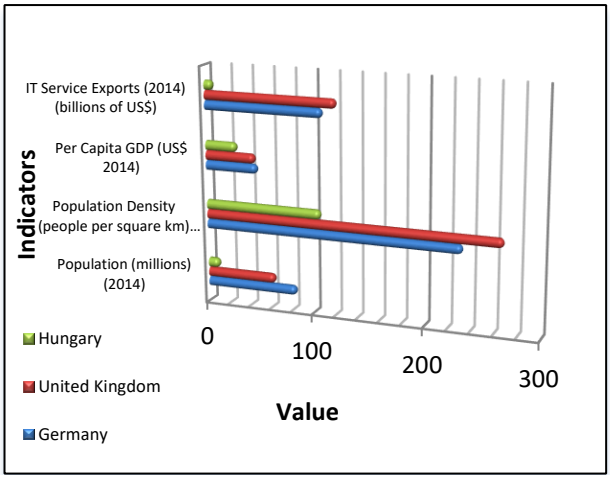

Figure 10: Population Indicator versus GDP

Based on (Table 2), figure 10 shows the population of each country compared to the population density per each square Kilometer, which gives us a general perception of the difficulty of delivering internet services according to the population census and also maintaining the security of information without preventing penetration. On the other hand the graph shows the differences in the expected growth of the average real GDP per capita compared to the total annual export volume for 2014 in IT services taking into account the services of cloud computing which is considered one of the leading services these days.

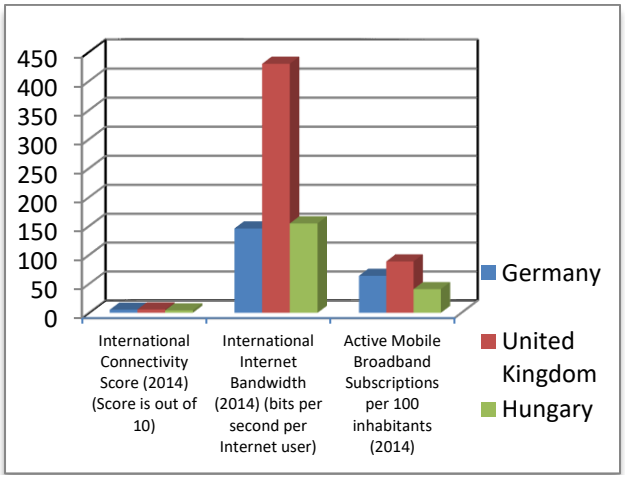

Figure 11: International Internet Bandwidth versus Connectivity score

The last diagram (Figure 11) also based on (Table 2) clarifies the total Active mobile broadband subscription percentage per each country where we can notice that United Kingdom took the first place by having the largest number of active mobile broad band subscriptions, keeping into consideration that it also had the first rank by adopting the highest international internet bandwidth as well as the international connectivity score in 2014, which gives us an indication regarding the reason of why UK is considered as one of the top leading countries in regulating and implementing such cloud computing services.

RESULTS

As we can notice from the Figures (2-8) above, there are 7 sections; each one have several answers' ratings regarding each country, as a result the average Values of the answers was calculated for each country aside, finally the Results were as the following:

- Germany total Ratio = (81.43%)
- Hungary total Ratio = (74.21%)
- United Kingdom total ratio = (83.21%)

Based on the targeted domains that was focused on during this study, the Above values clearly show that United Kingdom is considered as one of the leading countries concerning readiness and ability of implementing such cloud services, nevertheless we can notice that Germany highly compete and rise above UK in some major fields such as Data Privacy and Promoting Free Trade sections, also it is worth mentioning here that Data privacy part is considered as one of the most important requirements for a healthy implementation process of Cloud solutions and as it is noticeable due to the previous values; Hungary come over the other two competing countries in that regard, and simply defeats Germany in two other fields (Security and cybercrime).

CONCLUSION

Nevertheless Cloud computing is a serious essential and useful trend in recent times but most of the users underestimate its riskiness , however it should be so clear that cloud computing is divided into several main kinds, most important ones are the Public cloud, hybrid cloud , community cloud and private cloud, and for a simple declaration, Public cloud concept mostly is being incarnate in (SAAS) model "software as a service" where the service provider controls all of the elements in the cloud model, while Hybrid cloud could be similar to the IAAS "Infrastructure as a service" and PAAS "Platform as a service" models where the institution and service provider share the responsibility of controlling the cloud elements, at last the Private cloud which is considered as the most secured option since it is created and managed by the institution itself, nevertheless that this methodology ensure effectiveness and more security but it wouldn't actualize one of the main goal of expenses reduction which should be materialized by using cloud notion .

However, there are some key points that most of the authorities agreed on to help institutions ensure constant and secure work procedures for the use of cloud computing services, especially the outsourced ones.

One of the main points is to consider any relevant Regulatory obligations peculiar to Cloud computing services focusing on Jurisdiction as where the service provider is located, and guarantee the Effective access to Data and Premises by authorized people and regulators specifically on data related to the outsourced activities offered through service providers, moreover Contracts should ensure on the right of contacting the service provider directly in case firms cannot disclose data for any reason and ensure allowance to business premises which are relevant for the exercise of effective oversight if needed. Alongside, a focus was on Risk Management part which was defined as the processes of analyzing, assessment, controlling, and avoidance, minimization, or elimination of unacceptable risks, like wise institutions may use risk assumption, risk avoidance, risk retention, risk transfer, and any other strategy or combination of strategies in proper management of the future events, taking into account Business recovery in case of outsource provider failed, also not forgetting any Breach's notification in worst event of unwelcome intruders. On the other hand Security assessment and a Data residency policy with the provider should be carried out by a firm, but In case of using public clouding then Data segregation and Data sensitivity should be considered also, keeping into account the identification and appliance of Security classification by the institution to the data that is planned to be outsourced to the cloud service provider in line with the legal regulations and its own data protection rules, however the institution supposed to obtains assurance that the cloud service provider adheres to the relevant Data protection rules and legal regulations that are set by several authorities such as the

DPA in UK , BDSG in Germany and NAIH in Hungary to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. However, it is also essential for firms to have a comprehensive Change management process, establishing what provision has been made for making future changes to technology service provision and how the testing of changes will be carried out, also important to note that a regular assurance of the cloud service provider's full compliance with data security and protection requirements is recommended at least annually or after significant changes in the relevant business process, service, configuration or legal environment. Furthermore most of the opinions concentrated on the need of a Continuity plan which should be reviewed and adopted by the higher management in case of any disturbance in work flow or unexpected trouble and service provider failure, to maintain well functioning and healthy work procedures, also it is a must to have a documented, fully tested Exit plan to ensure the capability of exiting outsourcing plans without undue disruption to the firm's provision of services or t/he compliance with regulatory regime in case of termination or transition to an alternative service provider, focusing on the obligations in termination agreement that ensure outsourcing provider cooperate with the firm for a smooth transitions.

Finally, Based on that we can realize that there should be different rules that regulate such trends, thus in my opinion, a partnership between all concerned European countries is needed, to agree on a unified official party which should be responsible for setting up the regulations and standards that suits well the EU region especially for cloud computing, Due to the geographical proximity, unity situation and the possible need to exchange such services among EU countries based on the global well known standards, after that a classification and ranking for the fresh as well as the old cloud service providers should be done based on their sufficient compliance to those regulations and standards so by reviewing these ranks, it will be easier for the beneficiary organization to choose the best fit cloud service provider and contract with him, keeping into consideration the Jurisdiction risk of where the service provider is located is essential since that might enlighten the attention on the importance of differentiating between private sector and governmental sector in using cloud computing.

In fact, the data that might be used, transmitted and stored by the governmental sector definitely will be much sensitive, impressionable and eventful than the other ones which are used in private sector since it would affect the general safety criterion in a country, on the other hand also in private sectors it should be admitted that data which are used in some financial institutions such as banks, insurance companies are also much sensitive and significant than the ones that are used in ordinary institutions when using cloud service, this is why it is essential to classify the data which will be used in cloud service before the implementation phase regardless what kind of cloud model will be used, also in that case for institutions which are classified in the same group and share the same business interests I suggest to use community cloud computing model which would shares infrastructure between those several institutions from a specific community with common concerns, whether managed internally or by a third-party, and either hosted internally or externally.

FUTURE WORK

The process of risk assessment and risk control phase, which might be one of the most important phases that is considered as an ongoing task at least once a year due to its high effect on the cloud service lifecycle success regardless which type of cloud service is used, and I suggest that this shouldn't be a task done from one side based on the contractual agreement, but instead it should be done from both sides especially the institution's side, and it is necessary to make a way for the IT internal auditors in the organization to participate in the risk assessment and risk control procedures to assure the safeguard risk mitigation point and agree on the risk appetite of the institution. Noting that the theory of cloud computing relies genuinely on data transmission process which makes it more vulnerable, that it is why a lot of authorities such as DPA in UK, NAIH in Hungary, BDSG in Germany and others were concerned regarding Data protection and Data security, not just on the personal level of living people but also on the organizational level regardless what type of cloud is used, since most of the cloud service providers use multi tenancy infrastructure to reduce cost, so users on public cloud should be aware that their information could be stored in a shared infrastructure, that is why I suggest that cloud service provider should contractually agree to bear a financial burden in case of fraud occurrence according to his mistake or not adherence to the regulations as agreed, as well as a security assessment and data residency policy with the provider should be carried always out by the firm.

ABBREVIATIONS

UK: United Kingdom; MNB: Magyar Nemzeti Bank (central national bank of Hungary); FCA: Financial conduct Authority; PaaS: Platform as a Service; SaaS: Software as a Service; IaaS: Infrastructure as a Service; PRIN: Principles for business; EU: European Union; ISO/IEC 27018: The first international code of practice for cloud privacy; PII: Protection of personally identifiable information; PRA: Prudential Regulation Authority; BSI: Federal Office for Information Security; BDSG: German Federal Data Protection; Act L of 2103: Electronic Security of State and Local Government Bodies in Hungary; ICT: Information and Communication Technology; C5: Cloud computing compliance controls catalogue; DPA: Data Protection Authority; SA-01: The first section of security policies within the Cloud computing compliance controls catalogue; NAIH: The Hungarian national authority for data protection and freedom of information; FSMA :Financial Services and Markets Act; BSA: Global Cloud Computing Score card; GDP per capita: Gross Domestic Product by the country total population.

CONFLICT AND INTEREST

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

FUNDING

University of Debrecen- Hungary / Supports half of the payment fees - In case of submission to a gold open access journal.

DATA AVAILABILITY

All Data is available in the paper, nothing more is needed or to be declared.

ACKNOWLEDGEMENTS

I would like to thank Dr. Jozsef Gall for his help and guidance in this project.

REFERENCES

1. P. Joshi, "Clouds and big data: A compelling combination", In *2016 3rd International Conferene on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 2113-2118, 2016.
2. N. Gupta and S. Thakur, The factors affecting adoption of cloud computing technology in education institutions, *International Journal of Advanced Research in Computer and Communication Engineering*. vol. 3, no. 6, pp. 7229-7235, 2014. doi:
3. Global Cloud Computing Scorecard. Available online: http://cloudscorecard.bsa.org/2016/ (accessed on 9 November 2016).
4. Government Cloud Strategy. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf (accessed on 9 November 2016).
5. FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services. Available online: https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-%E2%80%98cloud%E2%80%99-and-other-third-party-it (accessed on 15 November 2016).
6. A Magyar Nemzeti Bank 2/2017. (I.12.), On the Usage of Social and Public Cloud Services. Available online: http://www.mnb.hu/en/publications (accessed on 10 October 2016).
7. Cloud Computing Compliance Controls Catalogue C5. Available online: https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue.html (accessed on 1 December 2016).
8. Opinion 05/2012 on Cloud Computing. Available online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (accessed on 11 November 2016).
9. B. Sosinsky, *Cloud Computing Bible*. Wiley Publishing Inc. , Indianapolis, Indiana, 2011.
10. Cloud Financial Services. Available online: http://www.eba.europa.eu/documents/10180/1228702/Session+2+-+Mario+Maawad+-+Cloud+Financial+Services.pdf (accessed on 28 November 2016).
11. Guidance on the Use of Cloud Computing. Available online: https://ico.org.uk/media/about-the-ico/documents/1042330/cloud-computing-guidance-for-organisations.pdf (accessed on 14 October 2016).
12. The NIST Definition of Cloud Computing, Special Publication 800-145. Available online: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf (accessed on 15 October 2016).
13. Cloud Security Strategies. Available online: http://www.eba.europa.eu/documents/10180/1228702/Session+2++-+Fabio+Gianotti+-+Cloud+Security+Strategies.pdf (accessed on 17 December 2016).
14. C. S. Mitchell, Outsourcing personal data processing in the cloud. Available online: http://www.chrismitchell.net/Talks/121108_rev.pdf (accessed on 17 Januarry 2017).
15. Cloud Computing & Your Legal Questions Answered. Available online: https://www.twobirds.com/~/media/PDFs/Expertise/IT/Cloud%20computing%20law%20interactive.pdf (accessed on 17 November 2016).
16. A. Marinos, G. Briscoe, Community cloud computing, in: Proceedings of Cloud

Computing: First International Conference (CloudCom 2009), Beijing, China, December 1–4, 2009.
17. M. Castro, B. Liskov, Practical byzantine fault tolerance and proactive recovery, ACM Transaction on Computer Systems 20 (4) (2002) 398–461.
18. A. Haeberlen, A case for the accountable cloud, in: 3rd ACM SIGOPS International Workshop on Large Scale Distributed Systems and Middleware, Big Sky Resort, Big Sky, MT, October 10–11, 2009.
19. K. Curran and S. Carlin, Cloud Computing Security, International Journal of Ambient Computing and Intelligence. vol. 3, no. 1, pp. 14-19, 2011. doi: 10.4018/978-1-4666-2041-4.ch002.
20. C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in: 29th IEEE Conference on Computer Communications (INFOCOM'10), San Diego, California, USA, March 14–19, 2010. 633
21. Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in: 14th European Symposium on Research in Computer Security (ESORICS'09), Saint Malo, France, September 21–23, 2009.
22. G. Karame, M. Strasser, S. Capkun, Secure remote execution of sequential computations, in: 11th International Conference on Information and Communications Security (ICICS'09), Beijing, China, December 14–17, 2009.
23. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al, A view of cloud computing, Communications of the ACM 53 (4) (2010) 50–58.
24. L. P. Willcocks, W. Venters, and E. A. Whitley, Cloud sourcing and innovation: slow train coming? A composite research study, Strategic Outsourcing: an International Journal. vol. 6, no. 2, pp. 184-202, 2013. doi:
25. W. Du, J. Jia, M. Mangal, M. Murugesan, Uncheatable grid computing, in: Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'04), Hachioji, Tokyo, Japan, March 24–26, 2004.
26 G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, Provable data possession at untrusted stores, in: Proceedings of the 14th 577 ACM Conference on Computer and Communications Security (CCS'07), Alexandria, Virginia, USA, October 28–31, 2007.
27. W. Venters and E. A. Whitley, A critical review of cloud computing: researching desires and realities, Journal of Information Technology. vol. 27, no. 3, pp. 179-197, 2012. doi:
28. V. Ratten, Continuance use intention of cloud computing: Innovativeness and creativity perspectives, Journal of Business Research. vol. 69, no. 5, pp. 1737-1740, 2016. doi:
29. M. Werfs, et al., Migrating software products to the cloud: An adaptive STS perspective, Journal of International Technology and Information Management. vol. 22, no. 3, pp. 37-54, 2013. doi:
30. M. B. Gawali1 and K. S. Subhash, Task scheduling and resource allocation in cloud computing using a heuristic approach, Journal of Cloud Computing: Advances, Systems and Applications. vol. 7, no. 4, pp. 16 pages, 2018. doi:
31. J. Damsgaard, W. J. Kettinger, and M. Lacity, From the Guest Editors: Special Issue on "The Business Payoff of Cloud Services", MIS Quarterly Executive. vol. 13, no. 4, pp. 2 pages, 2014. doi:
32. S. Marston, et al., Cloud computing — The business perspective, Decision Support Systems. vol. 51, no. 1, pp. 176-189, 2010. doi:
33. Outsourcing Functions of Cloud "Bank of England. Available online: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/report-on-outsourcing-functions-to-the-cloud-1 (accessed on 22 September 2016).

34. D. A. Battleson, et al., Achieving dynamic capabilities with cloud computing: an empirical investigation, European Journal of Information Systems. vol. 25, no. 3, pp. 209-230, 2016. doi:
35. C. Grönroos, A service perspective on business relationships: The value creation, interaction and marketing interface, Industrial Marketing Management. vol. 40, no. 2, pp. 240-247, 2011. doi:
36. G. Haibach, Cloud computing and European Union private international law, Journal of Private International Law. vol. 11, no. 2, pp. 252-266, 2015. doi: 10.1080/17441048.2015.1067994.
37. P. D. Hert, V. Papakonstantinou, and I. Kamara, The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection, Brussels Privacy Hub. vol. 1, no. 2, pp. 1-26, 2014. doi: 10.2139/ssrn.2542125.
38. A. Prasad and P. Green, Governing cloud computing services: Reconsideration of IT governance structures, International Journal of Accounting Information Systems. vol. 19, no., pp. 45-58, 2015. doi:
39. B. Zwattendorfer, et al., "Cloud Computing in E-Government across Europe", In Technology-Enabled Innovation for Democracy, Government and Governance. EGOVIS/EDEM 2013, Lec*ture Notes in Computer Science*,, Berlin, Heidelberg, pp. 181-195, 2013.
40. Security Framework for Governmental Clouds. Available online: https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds (accessed on 9 November 2016).
41. National Authority for Data Protection and Freedom of Information of Hungary, Opinion on Data Processing by Drones. Available online: https://www.naih.hu/files/opinion_data_processing_by_drones_2015_02_04.pdf (accessed on
42. Hungary- Financial Supervisory Authority Issues Circular for Hungarian Financial Institutions on the Use of Cloud Computing Technologies. Available online: https://iapp.org/news/a/2012-08-08-hungary-financial-supervisory-authority-issues-circular-for-hung/ (accessed on 10 December 2016).
43. Europe's Digital Progress Report (EDPR) 2017 Country Profile Hungary. Available online: http://ec.europa.eu/newsroom/document.cfm?doc_id=44310 (accessed on 22 April 2017).
44. Hungary Country Commercial Guide. Available online: https://www.export.gov/apex/article2?id=Hungary-Market-Overview (accessed on 14 April 2017).
45. World Development Indicators: The information society, Data Catalog. Available online: http://wdi.worldbank.org/table/5.12# (accessed on 25 May 2017).