İleri Teknoloji Bilimleri Dergisi
Journal of Advanced Technology Sciences
ISSN:2147-3455

SECURITY CONSIDERATIONS REGARDING TERMS AND CONDITIONS OF CLOUD SERVICE PROVIDERS

Ahmet EFE[1] Isamettin OMAK[2]

[1]Ankara Kalkınma Ajansı, İç Denetçi, Dr., CISA, CRISC, PMP, Ankara, Türkiye

[2]Yıldırım Beyazıt Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ankara, Türkiye

Abstract- Security is one of the biggest issues in the cloud-computing world. The customers may keep sensitive information on the cloud services and should trust to the service providers. Cloud service providers should comply with the legislations like data protection laws and should give confidence about their security policy. The terms and conditions document could give some clues about the security policies of the providers. Therefore, in this study we reviewed the T&C documents of some cloud service providers from security aspect in order to provide key measures against breaches in the cloud environment.

Keywords- Cloud computing security, IT outsourcing, GDPR, terms and conditions, privacy policy

BULUT HİZMET SAĞLAYICILARININ HÜKÜM VE KOŞULLARINDA SİBER GÜVENLİKLE İLGİLİ HUSUSLAR

Özet- Güvenlik, bulut bilişim dünyasındaki en büyük sorunlardan biridir. Müşteriler bulut hizmetleriyle ilgili hassas bilgileri tutarlarken servis sağlayıcılarana tam güvenmek durumunda kalmaktadırlar. Bulut servis sağlayıcıları, veri koruma yasaları gibi mevzuatlara uymalı ve güvenlik politikaları hakkında güven tam vermelidir. Şartlar ve koşullar belgesi, sağlayıcıların güvenlik politikaları hakkında bazı ipuçları verebilmektedir. Bu nedenle, bu çalışmada, bulut ortamındaki ihlallere karşı kilit önlemler almak için bazı bulut servis sağlayıcılarının T&C belgelerini güvenlik yönünden inceledik.

Anahtar Kelimeler- Bulut bilgi işlem güvenliği, BT dış kaynak kullanımı, GDPR, şartlar ve koşullar, gizlilik politikası

1. INTRODUCTION

Cloud computing is a type of service that enables sharing computer resources (hardware and software). The companies, which maintain and supply the resources to users, are called service providers. In addition, the users are the customers who pay the service providers for using their services. These resources may be very flexible and multivariate according to user needs. Because the target group of cloud services can be vary widely; different types and different sizes of companies, state agencies or even single users.

Cloud computing is a type of distributed computing. In this type of computing the service providers connect multiple and physically distributed devices as a single coherent system. This is transparent for users who make use of it. That means the users cannot see all parts of the system in detail. Virtualization technology is used to make the system transparent.

Another attribute of the cloud computing is location independency. This attribute is an advantage both from customers and providers perspective. The advantage for customer is that the system can be accessed from anywhere - anytime, for providers the maintenance and scalability can be achieved easily with this attribute.

There are mainly three types of cloud service models to meet different costumer's demands [1]:

Software as a Service (SaaS): This is the lightest type of service. The user has very limited control over the system. There is software supplied by the provider and the user given a role to change limited settings of this software.

Platform as a Service (PaaS): In this type of service the system used as a platform to develop some applications by the consumers. The consumers have control over these applications but not over the infrastructure of the system.

Infrastructure as a Service (IaaS): Users can access to the fundamental computer resources such as computation power, storage and network. Users allowed running and managing advanced applications which include operating systems or system applications.

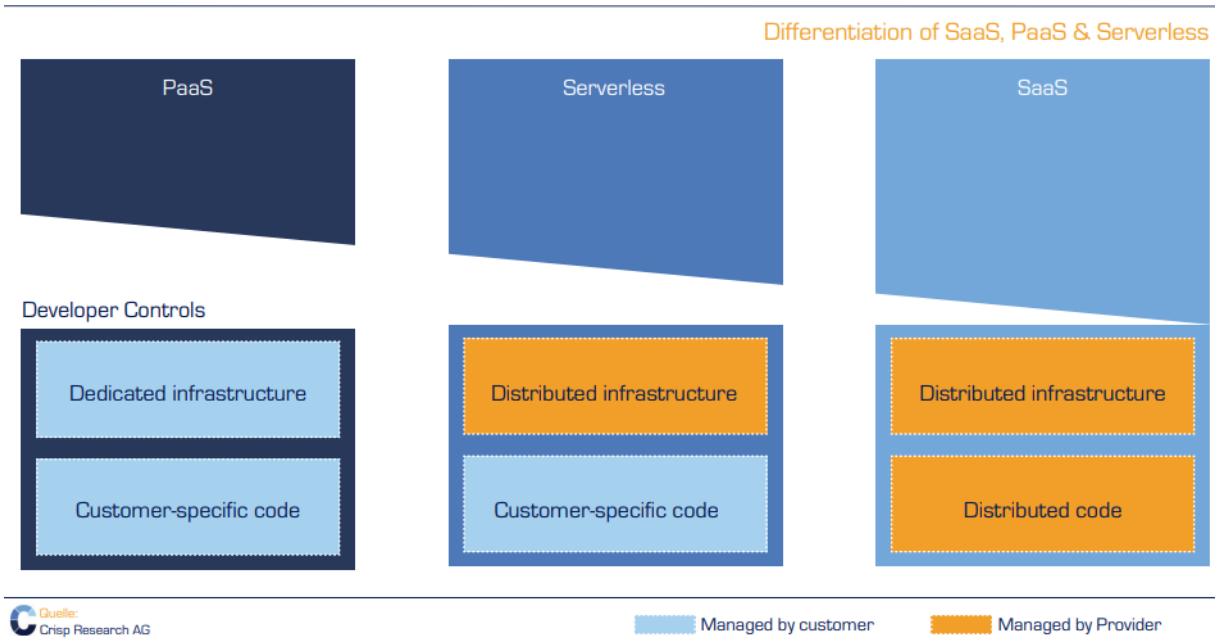


Figure 1. Differentiation of SaaS, PaaS and Serverless Cloud Infrastructures [26]

Besides these services, there are different specific types of services given below:

Identity as a Service (IDaaS): This is a new model in cloud computing. In this type of service, authentication or identity management supplied to the user by the service provider [2].

Mobile Backend as a Service (MBaaS): This type of cloud service provides solutions to meet the needs of mobile application development. The mobile application developers can use the infrastructure with all up to date features of mobile devices and can manage and run properly their applications on this service.

Intrusion Detection System as a Service (IDSaaS): This service aims to use an Intrusion Detection System on the cloud infrastructure which maintained by the costumer to secure the cloud environment.

Backup as a Service (BaaS): Provide online backup and recovery tools connected with clouds.

Disaster Recovery as a Service (DRaaS): Provide failover systems that applicable to the cloud to keep the system works correctly.

On the deployment aspect cloud computing separated into four models [1]:

Private Cloud: The cloud service is specified to a single organization to meet different needs.

Community Cloud: The cloud service is used by a specific community from multiple costumers with similar or common purposes.

Public Cloud: The cloud service is open for use of general public.

Hybrid Cloud: The deployment type is made of two or more different models above.

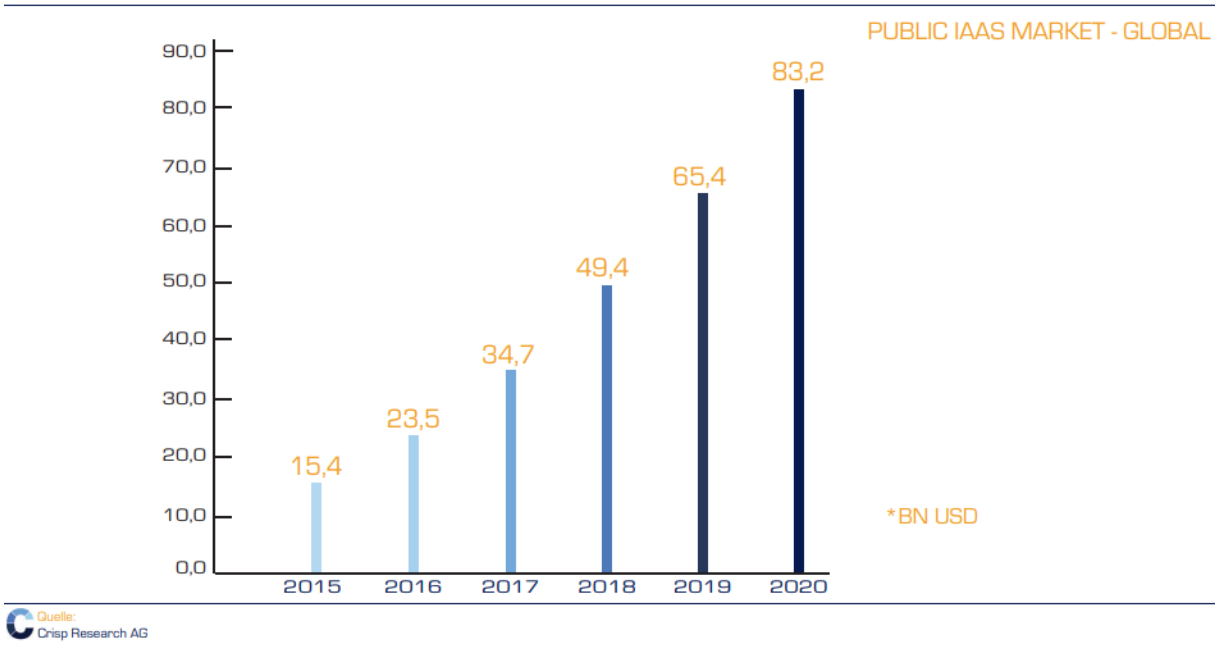


Figure 2. Up-Trending Cloud Market Value [26]

When organizations or individuals use cloud instead of purchasing the hardware they gain some advantages like; reducing costs, easily maintaining the system, using the resources that they exactly need, easily scaling the system. No need for a building which physically includes the hardware, cooling systems, experts for maintaining the system and so forth.

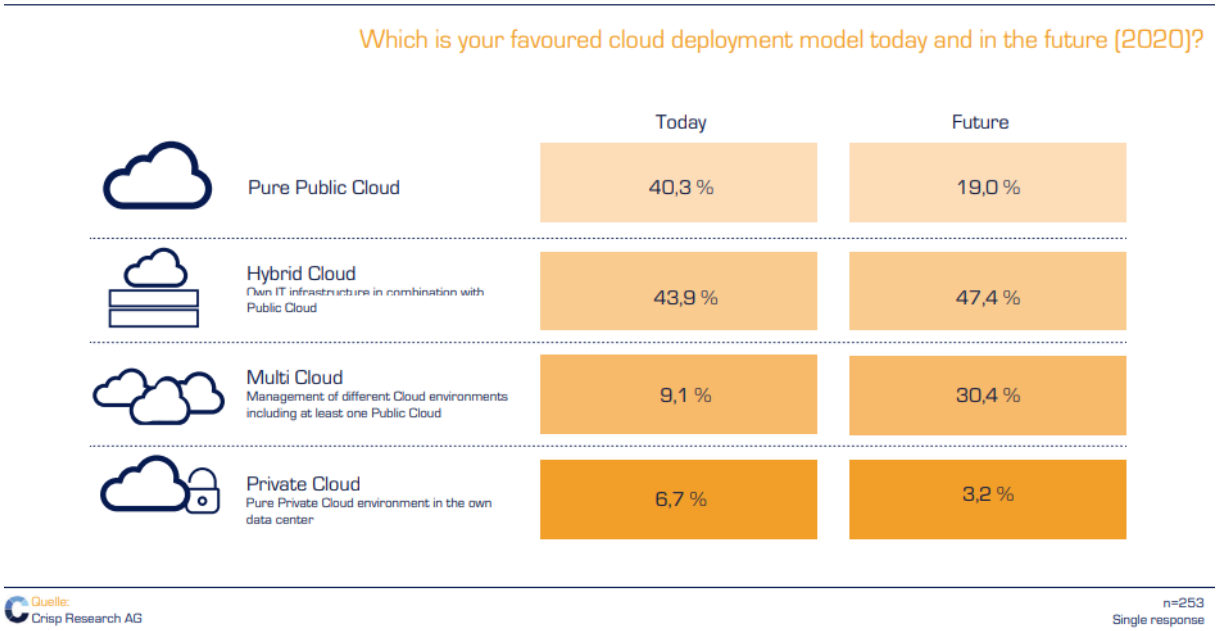


Figure 3. Future Projection for Different Cloud Infrastructure [26]

Due to all these advantages, its use is increasing day by day. With this widespread use, the security risks are an important issue that should be taken into account. Unauthorized accesses to the system or any other failures in the system can cause serious problems related to security like; preventing users from accessing their own data, lose a part or all of the data. Privacy is another challenge related to the security. This challenge refers to

privacy of the data kept in the cloud and privacy of personal information given by the user or collected by the provider whiles the use of the system. Customers need to know how the service provider use their information and how protect the information from unauthorized access and theft. Because of the transparency, customers usually do not have detailed information about the components of the service. Consequently, security risks must be eliminated with mutual confidence [3]. The terms & conditions (T&C) of cloud services should give this trust to the customers. However, because these documents are often complex and lengthy, the content cannot be analyzed as required by users. Most of the users do not read these documents and it is not easy to understand them. When a customer wants to decide which service provider supplies better security in their services looking at and comparing the T&C documents could be helpful. This paper would be a guide for these cases. In this study, our aim is to analyze, categorize and compare the T&Cs of some specified cloud service providers from the security aspect. Moreover, cloud computing as IT outsourcing and the legislation in the field of personal data will be covered to in this study.

2. MATERIALS AND METHODS

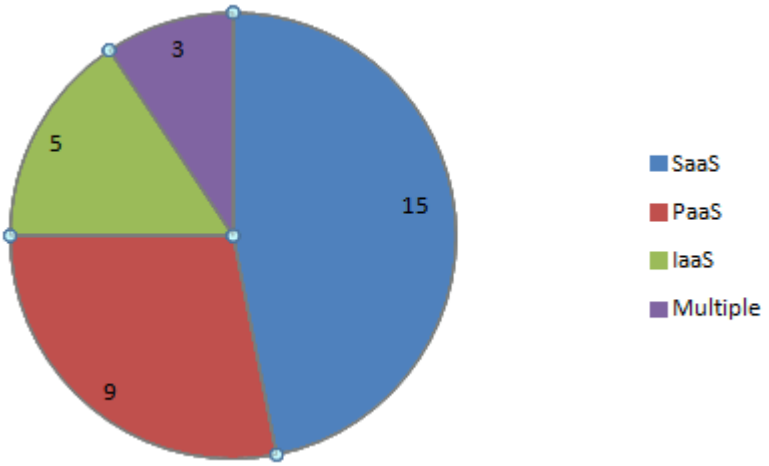
This study starts by giving general information about cloud computing defining the problem and the aim, which is already done in the introduction section. The next step is reviewing the literature about security in cloud services, IT outsourcing and legislation. After that the web sites of the cloud service providers will be reviewed to see the given promises on security to the potential customers. The sign up procedures for each service provider will be examined. Then the T&Cs will be analyzed in details from the security aspect and legislation, categorized and compared with each other, with the promises given in the web sites by the providers and with the given responsibilities to them in the law. At the end of the study we will come up to a conclusion about T&C documents of cloud computing and we will be mentioning about future work ideas to continue this study.

3. CLOUD CONTRACTS: UNDERSTANDING PROVIDER'S TERMS

There exists a study in 2010 [23] that compare and analyses the T&C documents from 27 different providers. According to that study the T&C documents differ as the version of service; Paid or free, the nature of service; SaaS, PaaS or IaaS, type of customer; Consumers, Small/Medium Enterprises and Corporate / Public Administration [23]. That study mentions that the T&C documents generally include Terms of Service, Service Level Agreement, Acceptable Use Policy and Privacy Policy; and in the same study, T&C documents categorized under 20 different subjects [23]. According to Wikipedia, there are 267 pages under cloud-computing provider's category [24]. However, some of these pages refer to same parent organization like Microsoft, Microsoft Azure, Microsoft Azure Web Sites, and Microsoft Egypt. If we exclude this type of pages, the total count reduces to about 240.

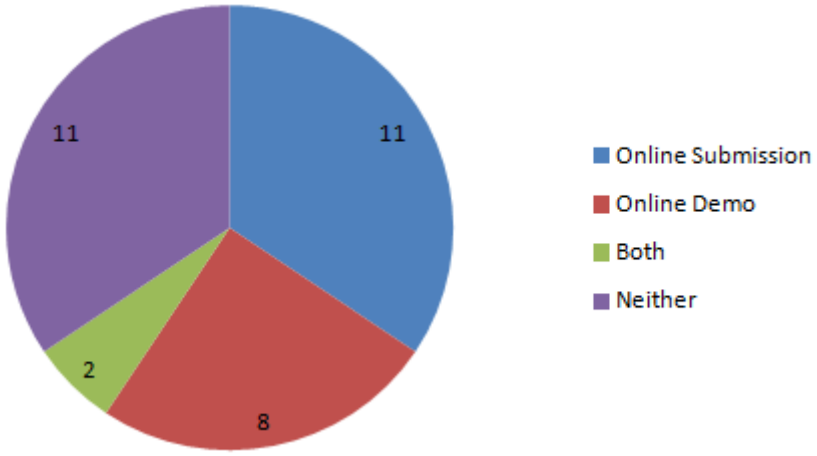
We reviewed 32 different cloud service providers in this study. When we categorize them by type of the service, the results are as in the chart of Figure 3. Three of them have more than one type of service; one with SaaS, Paas and two with Saas, Paas, Iaas

Figure 4: Cloud service providers categorized by type of the service



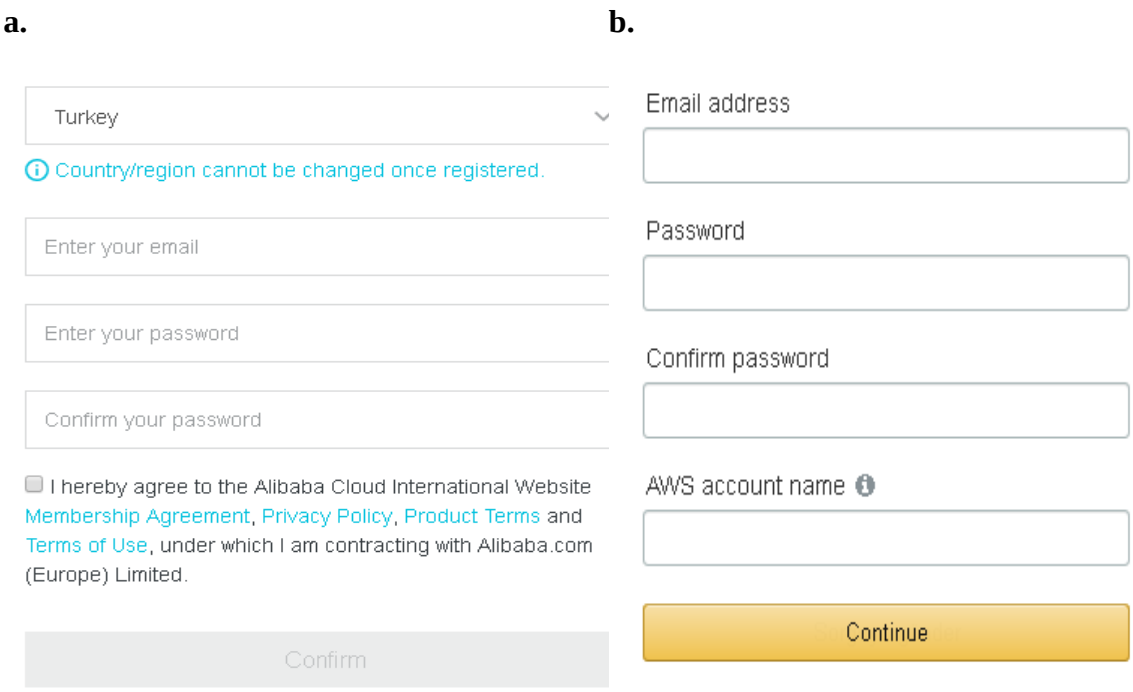
After that, we looked at each provider if it has online submission option and/or online demo and the results for these options are as shown in the Figure 5.

Figure 5: Cloud service providers categorized by online submission and demo options



Furthermore, we reviewed the providers with online submission option if they have any expression like a link or check box about license agreement as in the Figure 6. We saw that seven of the 13 provider have no any statement on the submission step.

Figure 6: An example for online submission form a- with and b- without the license agreement option



The T&C documents have different types and in some cases same types named differently. All types and names of the T&C documents collected from these 32 providers web sites are as in the following list: Acceptable Use Policy, Candidate Privacy Statement and Arbitration Agreement, Code of Ethics, Customer Agreement, End User Licence Agreement, End User Terms of Service, Legal, Legal FAQ, Legal Notices, Libellous Statement Policy, Licence Agreements, Membership Agreement, Portal Terms of Use, Privacy and Legal Policy, Privacy Policy, Privacy Principles, Privacy Shield Policy Statement, Privacy Statement, Security Policy, Service Level Agreement, Service Terms, Site Terms, Terms and Conditions, Terms of Service, Website Product Terms of Service. 5 of the 32 providers have no any T&C document reachable from their web site. Most of them have Privacy Policy and Terms of Use documents.

The cloud computing market has evolved in recent years. The commercial offerings of service providers have become more flexible, and we have seen changes in providers' traditional 'take it or leave it' approach to cloud contract terms. However, although there's now more negotiation of cloud contracts, the key for organizations evaluating cloud solutions is to know which elements of contracts can be negotiated, and by how much. Here are some of the key issues to consider. Cloud computing services are generally implemented on the provider's terms - although it can often be a struggle to figure out exactly what those terms are. Watch out for some cloud providers' complex, multi-document contract structures that may be poorly updated and oddly worded. In particular, don't assume that you know what's in a provision based on its heading. For example, in some terms, 'force majeure' seems to be elastic-sided enough to capture "changes in the

taxation basis of services delivered via the Internet" as a force majeure event! Understandably, contracts for private cloud solutions and with system integrators/resellers allow more scope for negotiation than contracts with public cloud providers. However, even in public cloud deals, terms are increasingly negotiable - although the degree of negotiability certainly pales in comparison with traditional outsourcing contracts.

Some of the key issues that tend to recur in cloud contract negotiations include [25]:

• Customer control and visibility over subcontracting, with a general reluctance from providers to allow approval over, or even to identify, subcontractors;

• Limitations on the provider's ability to change the nature of the services. (Here it's generally advisable for customers to focus on the commercial implications of such changes, rather than the right itself);

• Privacy and data security commitments;

• Rights of the provider to suspend services, e.g., for non-payment or violation of an acceptable use policy;

• Limitations of liability; and

• Exit provisions allowing the customer to extend service for a period after termination or expiry to allow migration to the replacement solution.

Technical areas do not tend to lend themselves to negotiation given the commoditized nature of cloud solutions - and you can show your naivety by asking for changes that directly contradict the services model.

4. CLOUD CONTRACTS: 2. DUE DILIGENCE

Because of the constraints on your ability to negotiate the provider's cloud terms, it is essential to carry out appropriate due diligence on the provider. Areas of focus should include [25]:

- Location of services
- Service performance and usability
- Existing customers (references)
- Data location, processing, portability and recovery
- Security
- Interoperability
- Business continuity
- Exit

5. CLOUD CONTRACTS: THREE - DATA PRIVACY REMAINS CENTER STAGE

Security is one of the most important issues in the world of cloud computing. Since the organizations and individuals transfer sensitive information into the cloud environment, naturally they want to make sure that their data is safe in the cloud and the environment of the cloud computing system is confident [4]. As the users have very light management

privileges over the system of the cloud they have to trust the provider but still every user should be aware of the vulnerabilities, risks and threats related to uses of the cloud and how trustworthy the system is.

The study [5] specify 28 different security issues and put them into categories as: "security standards, network, access control, cloud infrastructure, data" [5]. "Lack of auditing, lack of legal aspects, trust, network security configurations, internet dependence, account and service hijacking, browser security, insecure interface of API, security misconfiguration, server location and backup, data recovery, data privacy, data availability" is some of these issues identified in [5]. Features of the cloud computing cause security risks in addition to the conveniences. The high availability increases vulnerabilities again some threats such as Distributed Denial of Service (DDoS) attacks [5].

[6] evaluates security issues in trust and identification of threats concepts and suggest employing a trusted third party within cloud environment as a solution [6]. In [7] the authors remark security issues in a hierarchical way and split them as deployment model, service model and network related issues. The authors evaluate deployment model related issues in [7] as; "cloning and resource pooling, motility of data and data residuals, elastic perimeter, shared multi-tenant environment, unencrypted data, authentication and identity management"; service model related issues as; "data leakage problems, malicious attacks, backup and storage, shared technological issues, service hijacking, virtual machine hopping"; network related issues as; "browser security, SQL injection attack, flooding attack, incomplete data deletion, locks in". In a paper published by ISACA they mention some risks in the cloud computing field, how to come up with that risks, governance and assurance perspective of cloud computing [8]. In that paper "transparency, privacy, compliance, trans-border information flow, certification" examined as key assurance issues that need to be addressed [8]. Verma & Tyagi briefly review cloud computing security in three categories; "data security, data storage security, hostile attack" [9]. Wei et al. recommend a protocol called SecCloud which task is securing data storage and computation, preventing privacy cheating and providing efficiency [10]. Sun et al. describe security issues in three categories; "security, privacy and trust issues"; and sub categories for each of these main subjects [4]. Westphall et al. propose a monitoring tool for cloud computing security that uses data and logs [11].

It is also vital to understand how responsibility for data privacy obligations will be allocated between you and the provider, including who is responsible for data security. Typically, providers have been more willing to take on responsibility for network integrity, while trying to avoid obligations in relation to security of the data itself. However, over recent years, cloud service providers have been improving their privacy offerings. For example, there has been an increased willingness of providers to adopt the EU model clauses for data transfer. In addition, many providers now offer European-based data centers, reacting to commercial pressures from Europe-based clients.

When evaluating cloud solutions:

• classify the data concerned (including its sensitivity), and consider what would happen if data was disclosed, lost or corrupted;

• consider what the business impact would be if you were unable to use the data;

• check whether the provider is compliant with ISO/IEC 27001/2 and, if a public cloud provider, ISO/IEC 27018; and

• ensure that your deployment of cloud will comply with applicable data protection law, taking into account all relevant regulatory guidance, e.g., the EU Data Protection Working Party 29's opinion on cloud, the EU Cloud Standardization Guidelines and the ICO's guidance on cloud computing[25].

In cloud computing, every component is online, which exposes potential vulnerabilities. Even the best teams suffer severe attacks and security breaches from time to time. Since cloud, computing is built as a public service; it is easy to run before you learn to walk. After all, no one at a cloud vendor checks your administration skills before granting you an account: all it takes to get started is generally a valid credit card.

6. CLOUD CONTRACTS: FOUR - PERFORMANCE COMMITMENTS ARE HARD TO FIND

At the present time IT investments are among the most crucial operations for any type of organization. Performance of the company and the profit are mostly related to IT usage. Traditionally, companies have met their IT needs through direct purchases. But later on, to lease that need from another provider for a certain period of time has arisen as a new way of IT investment and called IT outsourcing. Barry Derksen examines IT outsourcing from business alignment aspect and found that IT outsourcing has no negative but a slightly positive effect on alignment [12]. Companies use IT outsourcing to be successful and to attain benefits from the process. In the paper [13] the authors define 18 key factors to be successful in IT outsourcing as; "Commitment from top management, Clear aims and Objectives, Capability to conduct, Confidence, Comparative treatment, Contract scale, Contract flexibility, Connection at the top, Cultural Fit, Communication, Calibre of the company, Competence, Clearly defined roles, Client knowledge, Consistency, Continuous improvement, Customer focused, Continuity and succession planning" [13]. Schlosser et al. define a relationship between internal businesses and a successful IT outsourcing; to get more benefits from IT outsourcing a good internal IT alignment is needed [14]. Goo et al. studied the impact of service level agreement to the preference of an IT outsourcing provider [15]. In that study, the authors define three types of service level agreement characteristics; "Foundation characteristics, change characteristics and governance characteristics" [15]. Today cloud computing is one of trend outsourcing type. Using cloud as an IT outsource is easy and fast from the entrepreneurs' perspective. However, organizations still should care about security of the cloud services they provide [16] and about the privacy of their information kept on the cloud environment.

Ensure that you are comfortable with the level of service performance commitment offered by the cloud provider. Most cloud contracts remain light in terms of service levels, with availability being the typical measurement metric. Check the wording of the SLAs carefully – watch out for references to 'service levels designed to be available', 'target service levels', etc. Also, identify the remedies available for service failure – it is common for providers to offer credit for additional services, despite the fact that it is hard to see 'more of the same' as a valuable remedy [25].

7. CLOUD CONTRACTS: FIVE - REGULATORS ARE TAKING NOTICE

Cloud service providers should not be contrary to the law while supplying resources. Since they serve overseas, from cloud service provider perspective it is a very difficult

task to be compatible with different types of law documents constructed by and valid in different countries. Thus, the organizations that use cloud services should be aware of the alignment between providers and legislation in that field. Below we covered some of the law documents related to cloud services.

7.1. EU-GDPR

General Data Protection Regulation (GDPR) [17, 18] is a regulation for companies including cloud service providers while giving service in EU countries. This regulation was approved on 14 April 2016 by the EU parliament and the application date is 25 May 2018 [17]. If an organization based in the EU or collects and processes data from EU citizens, it should comply with the GDPR. This document consists of 11 chapters and 99 articles separated by subjects. In Table - 1 of Appendix-A you can see a table, which is a list of all the articles with their titles.

7.2. FINAL REPORT ON RECOMMENDATIONS ON CLOUD OUTSOURCING

This report is another legislation document, which is more specific to clouds in banking sector published by European Banking Authority [19]. The guidance is on the use of cloud service providers by financial institutions. The guidance, which is applicable as of July 01, 2018, is addressed to credit institutions, investment firms, and competent authorities [20]. In Appendix-B, you can find a hierarchic list of the titles of this report.

7.3. PRIVACY SHIELD FRAMEWORK

This is a program that defines regularities to protect personal data while transferring from the European Union and Switzerland to the United States [21]. This program is created by the U.S. Department of Commerce, and the European Commission and Swiss Administration. In Appendix-C, you can see a hierarchic list of the titles of this framework.

7.4. THE LAW OF PROTECTION OF PERSONAL DATA IN TURKEY:

As of most countries, Turkey has also its data protection law document, which is published in 7 April 2016. The purpose of this law is to protect the fundamental rights and freedoms of persons, in particular the confidentiality of private life, in the processing of personal data, and to regulate the procedures and principles that they will comply with the obligations of real persons and legal persons who process personal data [22]. In Appendix-D, you can see a hierarchic list of the titles of this law.

If you are a regulated entity, you will need to take account of relevant regulatory guidance. This high-level guidance is aimed at ensuring regulated firms appropriately identify and manage risks relating to the deployment of cloud-based solutions. Issues identified in the guidance include [25]:

• Legal and regulatory considerations

• Risk management

• Oversight and audit

• Data privacy and security

• change management

• Business continuity

• Exit

8. CONCLUSION AND FUTURE WORK

Ultimately, you need to approach cloud transactions with a heavy dose of pragmatism, accepting that it may be very difficult to negotiate material changes to a cloud provider's terms. You need to carry out a thorough risk/benefit analysis exercise in order to evaluate whether the particular cloud solution is right for your business. If you perceive the risks to be so great that significant contract negotiation seems essential before putting services in the cloud, it may be that cloud is not the right solution for you after all.

In this study, we have reviewed the T&C documents of some cloud service providers. We saw that the providers have different types of T&C documents on their web sites; some of them have no any T&C document reachable from their web site. This study is uncompleted because the different types of documents from each provider should be reviewed in details and the number of the included providers should be expanded.

In this article, we have tried to provide an overview of the state of the various platforms available on the market for cloud-based systems based on terms of references. We had the opportunity to review the historical transformation of cloud-based software development tools from simple code editors to modern programming environments that could cover more than one stage in the development cycle. Many of these platforms focus on delivering different tools to use a variety of languages in file version control, using extraneous file environments on the programming version. On the other hand, the deployment of cloud-based applications appears to be at a very early stage, based on the latest virtualization techniques and technologies. These technologies require special cloud systems management skills that most development teams do not have. It is very difficult to perform auditing, control and debugging from a generalized platform. Each programming language can offer tools that are different and not aware of cloud environments. In addition, modelling techniques and tools required in the analysis stage are not included as part of integration into third-party cloud modelling tools.

To ensure security consideration, one should consider some key measures as such:

- Looking out for structured processes, effective data management, good knowledge management and service status visibility.
- Understanding how the provider plans to resource and support continuous adherence to these standards.
- Making sure the provider's platform and preferred technologies align with your current environment and/or support your cloud objectives.
- Asking to evaluate the overall portfolio of services that providers can offer.
- Assessing the ability to protect data in transit through encryption of data moving to or within the cloud.

- Looking to understand the provider's data loss, breach notification processes, and ensure they are aligned with your organisation's risk appetite and legal or regulatory obligations.
- Ensuring user access and activity is auditable via all routes and get clarity on security roles and responsibilities as laid out in the contacts or business policies documentation.
- Asking for internal security audit reports, incident reports and evidence of remedial actions for any issues rose.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," September 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final .

[2] "What is IDaaS? Understanding Identity as a Service and Its Applications," Okta Inc., [Online]. Available: https://www.okta.com/identity-101/idaas/ . [Accessed 28 March 2018].

[3] Cloud Computing Compliance Controls Catalogue (C5), Federal Office for Information Security, Germany, 2016.

[4] D. Sun, G. Chang, L. Sun and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," Procedia Engineering, no. 15, 2011.

[5] I. Khalil, A. Khreishah and M. Azeem, "Cloud Computing Security: A Survey," Computers, no. 3, pp. 1-35, 2014.

[6] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, no. 28, 2012.

[7] M. H. Parekh and D. R. Sridaran, "An Analysis of Security Challenges in Cloud Computing," International Journal of Advanced Computer Science and Applications(IJACSA), vol. 1, no. 4, 2013.

[8] "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives," ISACA, 2009.

[9] D. Verma and R. Kumar Tyagi, "Cloud computing security: A Review," 2018.

[10] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Information Sciences, no. 258, 2014.

[11] C. Westphall, C. Merkle Westphall, R. Weingärtner, D. dos Santos, P. Fernando da Siva, P. Vitti and K. Vieira, Challenges in Cloud Computing Security, 2014.

[12] B. Derksen, Impact of IT outsourcing on Business & IT alignment, Amsterdam: Vrije Universiteit Amsterdam, 2013.

[13] I. Alessio and B. Rebecca, "The 18C's model for a successful longterm," Industrial Marketing Management, no. 41, 2012.

[14] F. Schlosser, H.-T. Wagner, D. Beimborn and T. Weitzel, "The Role of Internal Business/IT Alignment and IT Governance for Service Quality in IT Outsourcing Arrangements," in Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010.

[15] J. Goo, R. Kishore, H. Raghav Rao and K. Nam, "The Role of Service Level Agreements in Relational Management of Information Technology Outsourcing: An Empirical Study," MIS Quarterly, no. 33, pp. 119-145, 2009.

[16] J. McKendrick, "Cloud May Be The New Outsourcing, But The Same Due Diligence Must Apply," Forbes Media, 18 October 2014. [Online]. Available: https://www.forbes.com/sites/joemckendrick/2014/10/18/cloud-may-be-the-new-outsourcing-but-the-same-due-diligence-must-apply/#360d88dd1079 . [Accessed 30 March 2018].

[17] "EU GDPR," [Online]. Available: https://www.eugdpr.org/. [Accessed 2 April 2018].

[18] "General Data Protection Regulation GDPR - Final text neatly arranged," Intersoft Consulting, [Online]. Available: https://gdpr-info.eu/ . [Accessed 31 May 2018].

[19] "FINAL REPORT ON RECOMMENDATIONS ON CLOUD OUTSOURCING," Europian Banking Authority, 20 December 2017. [Online]. Available: http://www.eba.europa.eu/documents/10180/2170121/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf . [Accessed 31 May 2018].

[20] "EBA Publishes Final Report on Recommendations on Cloud Outsourcing," Moody's Analytics, 20 December 2017. [Online]. Available: https://www.moodysanalytics.com/regulatory-news/dec-20-eba-publishes-final-report-on-recommendations-on-cloud-outsourcing . [Accessed 31 May 2018].

[21] "Privacy Shield Framework," [Online]. Available: https://www.privacyshield.gov . [Accessed 2 April 2018].

[22] "KİŞİSEL VERİLERİN KORUNMASI KANUNU," 7 April 2016. [Online]. Available: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf . [Accessed 31 May 2018].

[23] S. Bradshaw, C. Millard and I. Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services," Queen Mary University of London, 2010.

[24] "Category:Cloud computing providers," Wikipedia, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Category:Cloud_computing_providers . [Accessed 5 April 2018].

[25] Baker, McLean, (2016), "Five key legal considerations when negotiating cloud contracts", Computerworld, https://www.computerworlduk.com/cloud-

computing/5-key-legal-considerations-when-negotiating-cloud-contracts-3637604/

[26] CRISP, (2017) "Cloud Computing Vendor & Service Provider Comparison", Vendor Universe, https://www.reply.com/Documents/Crisp_Vendor_Universe_Cloud%20Computing_250118_REPLY_englischeVersion_FINAL.pdf

APPENDIX-A

Table - 1: The list of articles of the EU-GDPR

1	Subject-matter and objectives	51	Supervisory authority
2	Material scope	52	Independence
3	Territorial scope	53	General conditions for the members of the supervisory authority
4	Definitions	54	Rules on the establishment of the supervisory authority
5	Principles relating to processing of personal data	55	Competence
6	Lawfulness of processing	56	Competence of the lead supervisory authority
7	Conditions for consent	57	Tasks
8	Conditions applicable to child's consent in relation to information society services	58	Powers
9	Processing of special categories of personal data	59	Activity reports
10	Processing of personal data relating to criminal convictions and offences	60	Cooperation between the lead supervisory authority and the other supervisory authorities concerned
11	Processing which does not require identification	61	Mutual assistance
12	Transparent information, communication and modalities for the exercise of the rights of the data subject	62	Joint operations of supervisory authorities
13	Information to be provided where personal data are collected from the data subject	63	Consistency mechanism
14	Information to be provided where personal data have not been obtained from the data subject	64	Opinion of the Board
15	Right of access by the data subject	65	Dispute resolution by the Board
16	Right to rectification	66	Urgency procedure
17	Right to erasure (‘right to be forgotten’)	67	Exchange of information
18	Right to restriction of processing	68	European Data Protection Board
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	69	Independence
20	Right to data portability	70	Tasks of the Board
21	Right to object	71	Reports
22	Automated individual decision-making, including profiling	72	Procedure

23	Restrictions	73	Chair
24	Responsibility of the controller	74	Tasks of the Chair
25	Data protection by design and by default	75	Secretariat
26	Joint controllers	76	Confidentiality
27	Representatives of controllers or processors not established in the Union	77	Right to lodge a complaint with a supervisory authority
28	Processor	78	Right to an effective judicial remedy against a supervisory authority
29	Processing under the authority of the controller or processor	79	Right to an effective judicial remedy against a controller or processor
30	Records of processing activities	80	Representation of data subjects
31	Cooperation with the supervisory authority	81	Suspension of proceedings
32	Security of processing	82	Right to compensation and liability
33	Notification of a personal data breach to the supervisory authority	83	General conditions for imposing administrative fines
34	Communication of a personal data breach to the data subject	84	Penalties
35	Data protection impact assessment	85	Processing and freedom of expression and information
36	Prior consultation	86	Processing and public access to official documents
37	Designation of the data protection officer	87	Processing of the national identification number
38	Position of the data protection officer	88	Processing in the context of employment
39	Tasks of the data protection officer	89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
40	Codes of conduct	90	Obligations of secrecy
41	Monitoring of approved codes of conduct	91	Existing data protection rules of churches and religious associations
42	Certification	92	Exercise of the delegation
43	Certification bodies	93	Committee procedure
44	General principle for transfers	94	Repeal of Directive95/46/EC
45	Transfers on the basis of an adequacy decision	95	Relationship with Directive 2002/58/EC

46	Transfers subject to appropriate safeguards	96	Relationship with previously concluded Agreements
47	Binding corporate rules	97	Commission reports
48	Transfers or disclosures not authorised by Union law	98	Review of other Union legal acts on data protection
49	Derogations for specific situations	99	Entry into force and application
50	International cooperation for the protection of personal data	51	Supervisory authority

APPENDIX-B: The list of titles of Final Report on Recommendations on Cloud Outsourcing

1. Compliance and reporting obligations
    - Status of these recommendations
    - Reporting requirements
2. Subject matter, scope and definitions
    - Subject matter and scope of application
    - Addressees
    - Definitions
3. Implementation
    - Date of application
4. Recommendations on outsourcing to cloud service providers
    - 4.1 Materiality assessment
    - 4.2 Duty to adequately inform supervisors
    - 4.3 Access and audit rights
        - For institutions
        - For competent authorities
    - 4.4 In particular for the right of access
    - 4.5 Security of data and systems
    - 4.6 Location of data and data processing
    - 4.7 Chain outsourcing
    - 4.8 Contingency plans and exit strategies
5. Accompanying documents
    - 5.1 Draft cost-benefit analysis/impact assessment
        - A. Problem identification
        - B. Baseline scenario
            - Formalities required
            - Mandatory contractual clauses
        - C. Policy objectives
        - D. Assessment of the technical options
            - Introduction of the recommendations versus the status quo
            - Exhaustive and prescribed list of requirements versus non-exhaustive list
    - 5.2 Feedback on the public consultation
        - Summary of key issues and the EBA’s response

APPENDIX-C: The list of titles of Privacy Shield Framework

I. Privacy Shield Framework

I. Overview

II. Privacy Shield Principles

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement and Liability

III. Privacy Shield Supplemental Principles

1. Sensitive Data
2. Journalistic Exceptions
3. Secondary Liability
4. Performing Due Diligence and Conducting Audits
5. The Role of the Data Protection Authorities
6. Self-Certification
7. Verification
8. Access
    a. The Access Principle in Practice
    b. Burden or Expense of Providing Access
    c. Confidential Commercial Information
    d. Organization of Data Bases
    e. When Access May be Restricted
    f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access
    g. Repetitious or Vexatious Requests for Access
    h. Fraudulent Requests for Access
    i. Timeframe for Responses
9. Human Resources Data
    a. Coverage by the Privacy Shield
    b. Application of the Notice and Choice Principles
    c. Application of the Access Principle
    d. Enforcement
    e. Application of the Accountability for Onward Transfer Principle
10. Obligatory Contracts for Onward Transfers
    a. Data Processing Contracts
    b. Transfers within a Controlled Group of Corporations or Entities
    c. Transfers between Controllers
11. Dispute Resolution and Enforcement

12. Choice – Timing of Opt-Out
13. Travel Information
14. Pharmaceutical and Medical Products
    a. Application of EU Member State Laws or the Privacy Shield Principles
    b. Future Scientific Research
    c. Withdrawal from a Clinical Trial
    d. Transfers for Regulatory and Supervision Purposes
    e. "Blinded" Studies
    f. Product Safety and Efficacy Monitoring
    g. Key-coded Data
15. Public Record and Publicly Available Information
16. Access Requests by Public Authorities

Annex I (Binding Arbitration)

A. Scope
B. Available Remedies
C. Pre-Arbitration Requirements
D. Binding Nature of Decisions
E. Review and Enforcement
F. The Arbitration Panel
G. Arbitration Procedures
H. Costs

APPENDIX-D: The list of titles for The Law of Protection of Personal Data in Turkey

1. Purpose, Scope and Definitions
    - Purpose
    - Scope
    - Definitions
2. Processing of Personal Data
    - General principles
    - Processing conditions of personal data
    - Processing conditions for specialized personal data
    - Deletion, destruction or anonymization of personal data
    - Transfer of personal data
    - Transferring personal data abroad
3. Rights and Obligations
    - Disclosure responsibility of the data controller
    - Rights of the person concerned
    - Obligations related to data security
4. Application, Complaint and Records of the Data Controller
    - Application to the data controller
    - Complain to the committee
    - Procedures and principles of examination on complaints
    - Data controller records
5. Crimes and Misdemeanors
    - Crimes
    - Misdemeanors
6. Personal Data Protection Authority and Organization
    - Personal Data Protection Agency
    - Institutional tasks
    - Personal Data Protection Committee
    - Duties and authorities of the committee
    - Working principles of the committee
    - President
    - Formation and duties of the presidency
    - Personal Data Protection Specialist and expert helpers
    - Provisions regarding people and personal rights
7. Miscellaneous Provisions
    - Exceptions
    - Institutional budget and revenues
    - Modified and added provisions
    - Regulation
    - Transitional provisions

Force

Executive