An Analysis of Cloud Certifications' Performance on Privacy Protections

Tian Wang and Masooda Bashir
School of Information Sciences, University of Illinois at Urbana-Champaign, 501 E. Daniel St., Champaign, U.S.A.

Keywords: Cloud Computing, Privacy Protections, Cloud Certifications.

Abstract: Cloud computing is an evolving paradigm that changes the way humans share, store, and access their information in digital form. Although cloud computing offers tremendous benefits, it also brings security and privacy challenges. Certifications have been developed by governments and authorized organizations as a new approach to protecting users' information in the cloud. While the security controls in the certifications have been well established and widely applied, the privacy protections provided by certifications are still ambiguous and yet to be examined. In this study, we identified and selected four cloud certifications that are commonly used for certifying the security and privacy of cloud computing, and we evaluated their performance on privacy protections specifically to understand how privacy is treated in these certifications according to their existing controls. Our research reveals a lack of privacy controls in the current certifications and inadequate privacy-related content; even when present, such content is not clear or is difficult to distinguish from security controls. Results demonstrate that without having a set of baseline privacy protection criteria or standards, it is very challenging to determine cloud certifications' performance and adequacy for privacy protections. It also points to the urgent need for the development of a consistent and comprehensive privacy framework that can be utilized for such evaluations.

1 INTRODUCTION

Representing a new revolution in information technology (IT), cloud computing provides a novel approach for using and offering IT resources that anyone can access on demand via the Internet (Leymann & Fritsch, 2009). The implementation of cloud computing offers many potential advantages in the real world. For example, Internet of Things (IoT) devices collect information from various physical devices and virtual sensors, all of which provide a wealth of knowledge for improving personalized recommendations and customer experiences. Similarly, state and local governments can use data-analytic results collected from cloud-connected resources to make strategic decisions about the placement of traffic lights, the construction of new roads or bridges, and other future plans for smart cities (Perera et al., 2015).

However, although collecting and storing large amounts of data in the cloud can be a tremendous asset for any given organization, it can also pose many challenges to privacy-preserving data practices. In particular, big data analytics in cloud environments have implications for user privacy at all stages of the cloud computing process. The cloud data collected by IoT devices may collect users' personal and sensitive information, ranging from information on their health conditions to their financial status, by recording daily activities in a way that can violate users' privacy (Perera et al., 2015). Therefore, there is a pressing need to develop privacy-related policies and technologies that not only provide baseline protections but also unify standards and potential regulatory efforts to ensure a higher level of privacy-preserving data management techniques (Gahi & Mouftah, 2016).

Many different approaches have been developed and applied to improve information security and privacy in cloud computing, and one important approach is the use of certifications, which serve as a mechanism for self-assessment and mitigate the trust gap between organizations and users by providing assurance that a CSP is doing correct and appropriate things. A certification is like an "ethical handshake" indicating trust between the CSP and the certification authority. Display of certifications contributes to the ability of organizations to gain

Wang, T. and Bashir, M.
An Analysis of Cloud Certifications' Performance on Privacy Protections.
DOI: 10.5220/0010783200003120
In *Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)*, pages 299-306
ISBN: 978-989-758-553-1; ISSN: 2184-4356

public trust as well. In addition, certifications and standards can be applied to set the requirements for the assessment and selection of solutions that meet the expected levels of information assurance and data privacy throughout the world (Guilloteau & Venkatesen, 2013). From the point of view of information privacy in the cloud, a certification is a credential that confirms a CSP has achieved certain characteristics, qualities, and/or status by following some form of assessment or audit in accordance with established requirements or standards. Currently, some of the best-known and most-used certifications related to information security and privacy include ISO/IEC 27001, SOC2, C5, and FedRAMP. While some of those certifications (i.e., ISO) have been around for over a decade, some like the C5 and FedRAMP have appeared more recently.

However, the great diffusion and fast-moving development of cloud computing applications and services have brought new threats to both security and privacy of information, weakening the protection that existing standards can offer. Traditional baseline privacy protection mechanisms offered by standards and certifications do not adequately address the fast-paced growth of data analytics. Moreover, the line between privacy and security is sometimes blurry. Previous studies have evaluated the overall completeness of certifications with respect to the level of security protection that they provide (Di Giulio et al., 2017), but to the best of our knowledge, there has been no current or published research that examines the adequacy of the existing cloud computing certifications with respect to information privacy specifically. Privacy protections become even more difficult to achieve because data privacy competes with constraints related to transparency and accountability of organizational management systems (Gai et al., 2016). As the collection of personal data has exponentially increased, the number of data breaches has also risen resulting in privacy harms. Litigation is currently not an effective solution for privacy infringement. For example, the majority of data breach court claims have been unsuccessful, with courts reluctant to recognize a privacy harm without an economic loss (Solove & Citron, 2018).

Whie most frameworks blur the line between security and privacy, it becomes very difficult to distinguish whether the requirement is meant for security, privacy, or both based on previous literature study (Sharma et al., 2020). Therefore, it is important to evaluate how information privacy is handled and protected in various cloud certifications. In this study, we propose a scientific and systematic analysis of four certifications: ISO/IEC 27001, FedRAMP, SOC2, and C5. These four certifications are selected since they have been widely used in cloud computing evaluation (Di Giulio et al., 2017). For example, any CSP that provides cloud services to federal agencies is required to have a FedRAMP Authorization to Operate (ATO), and the C5 standard has been conceived as a guideline that CSPs could use to improve their cloud systems. To analyze the four certifications, all the controls (refer to the measures that provide information protection) are retrieved and evaluated. The goal of this study is to understand whether various types of privacy controls are provided or missing for each of the four common certifications mentioned above, and how the four certifications perform on privacy protections in general. We believe that the results from this study mark an important step towards identifying privacy protection weaknesses in the certifications and highlighting improvements needed to meet privacy requirements and ensure data protection.

2 LITERATURE REVIEW

This paper builds on previous research studies into privacy issues and protections in cloud computing. A review paper by Lar et. al (2011) provided an overview of the security and privacy challenges in public cloud computing, as well as considerations that organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment. Similarly, in their survey study, Kumar et al. (2016) introduced a detailed analysis of current cloud security and privacy problems, including various existing approaches related to data encryption and message authentication. The study also pointed out some issues and challenges in cloud data processing. Another review paper by Sun et al. (2014) explored questions that should be addressed when considering data security and privacy in cloud computing; for example, how to enable users to have control over their data in cloud, how to guarantee user data replications in a consistent state, and which party is responsible for ensuring compliance with legal requirements regarding personal information.

It is important for cloud certifications to address privacy considerations in their content and controls as an approach to enhance cloud data protection. Previous research by Kang et al. pointed out that personal information protections were missing in one cloud security certification (ISO) and suggested adding the measures covered by the Personal Information Protection Act (Kang & Kwon, 2019). The research study by Anisettic et al. (2018) proposed a cloud certification scheme based on the continuous verification of model correctness. To have a trustworthy certification process, the proposed scheme was expected to involve property authorization-based privacy and property storage confidentiality. Similarly, Karkouda et al. (2018) proposed a scheme that would guarantee data availability and confidentiality, minimize the dependency of CSPs, and enable data analytics in the cloud without post processing by the client.

As the client of cloud services, individual users also express their demands on the privacy protections provided by certifications. In a prior work, Teigeler et al. (2018) explained the concept of Customer Pressure, that customers will prefer to use cloud services from companies who participate in a continuous certification, and they demand the companies to meet continuously technical, security, and privacy requirements. Specifically, users showed their concerns on cloud storage privacy that they believed the service providers were responsible for data loss (Lansing et al., 2013). While privacy is one of the criteria for scaling and empirically ranking various quality and trust assurance for consumer cloud service (Ion et al., 2011), it is necessary for CSPs to develop appropriate techniques and implement privacy protections to gain users' trust. One of the methods proposed by Lins et al. (2016) is to involve automated monitoring and auditing techniques and transparent provision of audit relevant information to verify CSPs' ongoing adherence to certification requirements.

3 METHOD

The first step is to retrieve all the controls, which are the measures that protect the confidentiality, integrity, and availability of information, from the four certifications: ISO/IEC 27001, FedRAMP, SOC2, and C5. To improve overall understanding of privacy protections provided by the certifications, in this study, we evaluated each control in the four certifications based on its name, definition, and relevant content, and then identified the controls that may be relevant to privacy, either explicitly or implicitly. The controls in each certification were classified into three categories: explicit privacy controls, implicit privacy controls, and controls irrelevant to privacy. For each of the four certifications (ISO/IEC 27001, SOC2, C5, and FedRAMP), the number of controls under each category, as well as the field of privacy the control is related to (if applicable), were recorded for further comparison and evaluation.

3.1 Data Pre-processing

Before evaluating the controls in the certifications, we retrieved the full content of the four certifications that were examined and compared in this study. Although some of the certifications have the updated or more comprehensive version that may include privacy-related controls, considering the public availability, Table 1 described the version of each certification (published year) used for this study and total number of controls in each certification.

Table 1: List of the 4 certifications for this study.

Certification Name	Published Year	Total # of Controls
ISO/IEC 27001	2013	114
SOC2	2017	61
C5	2020	121
FedRAMP	2012	168

3.2 Explicit Privacy Controls

Explicit privacy controls are defined as controls that explicitly include the keyword "privacy" or other words/phrases directly refer to privacy in the control name, definition, or relevant content (i.e., supplementary information, additional requirements). Since there exist many words and phrases that may have a similar meaning to privacy, in addition to the word "privacy" itself, other terms "private", "confidentiality", "personal information", "data protection", and "data breach" were also included in the evaluation criteria.

After identifying the explicit privacy terms, we examined the full content of each control in the four certifications by running an automated Python script to detect the keywords, recorded the controls including the terms mentioned above as the explicit privacy controls, and then removed those controls from the original documents (the control would be excluded once it was classified into one of the categories since it cannot be both explicit and implicit).

3.3 Implicit Privacy Controls

Similar to the process of identifying explicit privacy controls, the first step was to create a list of terminologies that may imply privacy protections as the evaluation criteria for implicit privacy controls.

To retrieve the relevant terms, we searched for publicly available documents that may include any privacy-related words and phrases. The privacy-related terms selected for this study were drawn from multiple sources, including privacy glossaries, lexicon, and online public dictionaries. The selected sources included the following:

- Data Protection Authority (DPA) Glossary.
- International Association of Privacy Professionals (IAPP) Glossary of Privacy Terms.
- National Institute of Standards and Technology (NIST) Glossary.
- Rochester Institute of Technology (RIT) Standards Lexicon. Note that RIT Standards Lexicon was selected as a source considering the overlap between security and privacy.
- Online public dictionary: Merriam-Webster, dictionary.com, vocabulary.com.

After identifying sources, we reviewed the content for each documentation and recorded any potentially relevant privacy-related terms. A privacy term was selected if it appeared under a section of the content related to privacy (i.e., privacy requirements, privacy issues), or if it was from a source specifically developed for privacy (i.e., IAPP Glossary of Privacy Terms). We continued the process by identifying and collecting the terminology from other sections that may also imply privacy based on our understanding. For example, some terms were introduced under the cybersecurity category, but the definition of the term involved both security and privacy perspectives. We also reviewed online public dictionaries to collect any additional privacy synonyms by reading the definitions. After creating the initial list of privacy terms, four researchers examined the relevancy of each term, and determined if it should be included or removed from the list.

The finalized list included 83 privacy terms (including both words and phrases), which we used to identify implicit privacy controls in each certification. We ran an automated script for a second round to detect if the keywords from the finalized list were included in the controls. As with the process of defining explicit privacy controls, once the control was identified as implicit privacy controls, we recorded those controls and removed them from the original documents.

3.4 Controls Irrelevant to Privacy

After excluding the explicit privacy controls and implicit privacy controls in each certification, the remaining controls in each certification were automatically classified as controls irrelevant to privacy.

4 RESULTS

Table 2 shows the number of controls under each category and the percentage of such controls over the total number of controls for each of the four certifications.

Table 2: Overview of controls in each certification.

Certification	# of Explicit Controls	# of Implicit Controls	# of Controls Irrelevant to Privacy
ISO/IEC 27001	2 (1.75%)	13 (11.40%)	99 (86.84%)
SOC2	24 (39.34%)	12 (19.67%)	25 (40.98%)
C5	20 (16.53%)	37 (30.58%)	64 (52.89%)
FedRAMP	3 (1.79%)	14 (8.33%)	151 (89.88%)

A more detailed comparison of the four certifications based on the number of controls is shown in Figure 1. According to the results shown in the bar chart, SOC2 includes the highest percentage of explicit privacy controls, as well as the highest percentage of overall privacy-related controls, and C5 includes the highest percentage of implicit privacy controls. However, privacy-related controls are rarely identified in either ISO/IEC 27001 or FedRAMP.

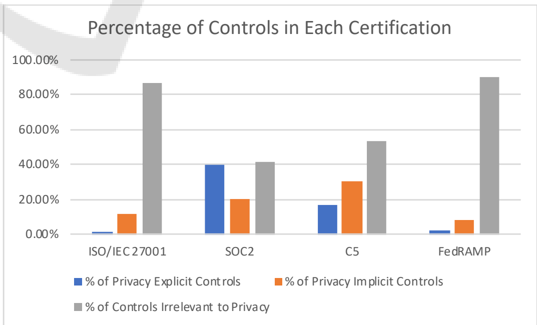

Figure 1: Percentage of controls in each certification.

4.1 ISO/IEC 27001

ISO/IEC 27001 includes 2 explicit privacy controls (confidentiality or non-disclosure agreements, privacy and protection of personally identifiable information) and 13 implicit privacy controls (listed in Table 3). The implicit privacy controls in ISO/IEC

27001 are related to access (access control, information and user access), authentication, collection, disclosure, disposal, and identification.

Table 3: Implicit privacy controls in ISO/IEC 27001.

Field related to privacy	**Controls**
Access control	Access control policy Secure log-on procedures Access control to program source code
Authentication	Management of secret authentication information of users Use of secret authentication information
Collection	Collection of evidence
Disclosure	Classification of information Securing application services on public networks
Disposal	Disposal of media Secure disposal or reuse of equipment
Identification	Identification of applicable legislation and contractual requirements
Information access	Teleworking
User access	User access provisioning

4.2 SOC2

SOC2 includes 24 explicit privacy controls. Examples of the explicit privacy controls are listed as below:

- C1.2 ("The entity disposes of confidential information to meet the entity's objectives related to confidentiality.")
- CC2.3 ("The entity communicates with external parties regarding matters affecting the functioning of internal control.")
- CC7.3 ("The entity evaluates security events to determine whether they could or have resulted…")
- CC7.4 ("The entity responds to identified security incidents by executing a defined incident…")
- CC8.1 ("The entity authorizes, designs, develops or acquires, configures, documents…")
- C1.1 ("The entity identifies and maintains confidential information to meet the entity…")
- P1.1 ("The entity provides notice to data subjects about its privacy practices to meet the entity…")
- P2.1 ("The entity communicates choices available regarding the collection, use, retention…")
- P3.1 ("Personal information is collected consistent with the entity objectives related to privacy.")
- …

SOC2 also includes 12 implicit privacy controls (shown in Table 4). The implicit privacy controls in SOC2 are related to access control, anonymity, disposal, data loss prevention, identification, risk assessment and management, and vulnerability.

Table 4: Implicit privacy controls in SOC2.

Field related to privacy	**Controls**
Anonymous	CC2.2 ("The entity internally communicates information, ...")
Identification	CC3.2 ("The entity identifies risks to the achievement of its objectives…") CC3.4 ("The entity identifies and assesses changes that could…")
Risk assessment	CC5.1 ("The entity selects and develops control activities that contribute…") A1.2 ("The entity authorizes, designs, develops or acquires, implements, …")
Access control	CC6.1 ("The entity implements logical access security software, …") CC6.3 ("The entity authorizes, modifies, or removes access to data, software, …")
Disposal	CC6.5 ("The entity discontinues logical and physical protections over …")
Data loss prevention	CC6.7 ("The entity restricts the transmission, movement, and removal of information to…")
Vulnerability	CC7.1 ("To meet its objectives, the entity uses detection and monitoring procedures to identify…")
Risk management	CC9.1 ("The entity identifies, selects, and develops risk mitigation…") CC9.2 ("The entity assesses and manages risks associated with…")

4.3 C5

C5 includes 20 explicit privacy controls. Examples of the explicit privacy controls include:

- Risk Management Policy
- Documentation, communication and provision of policies and instructions
- Confidentiality agreements
- Asset Classification and Labelling
- Capacity Management – Planning

- Data Protection and Recovery – Concept
- Logging and Monitoring - Metadata Management Concept
- Managing Vulnerabilities, Malfunctions and Errors -Penetration Tests
- …

C5 includes 37 implicit privacy controls (examples of controls are listed in Table 5). The implicit privacy controls in C5 are related to access control, appropriate safeguards, disclosure, encryption, identity, identification, risk assessment and management, surveillance, and vulnerability.

Table 5: Examples of implicit privacy controls in C5.

Field related to privacy	**Controls**
Access control	Authorization Mechanisms
Authentication	Authentication mechanisms …
Appropriate Safeguards	Version Control
Disclosure	Conditions for Access to or Disclosure of Data in Investigation Requests …
Encryption	Encryption of data for transmission (transport encryption) …
Identification	Logging and Monitoring - Identification of Events …
Identity	Policy for user accounts and access rights …
Risk Assessment	Risk assessment, categorization, and prioritization of changes …
Risk Management	Application of the Risk Management Policy …
Surveillance	Surveillance of operational and environmental parameters …
Vulnerability	Testing and Documentation of known Vulnerabilities

4.4 FedRAMP

FedRAMP includes 3 explicit privacy controls (Privacy Impact Assessment, Transmission Confidentiality, and Error Handling), and 14 implicit privacy controls (listed in Table 6). The implicit privacy controls in FedRAMP are related to access control, encryption, risk assessment, trust, and confidentiality.

Table 6: Implicit privacy controls in FedRAMP.

Field related to privacy	**Controls**
Access control	Access Control Policy and Procedures Access Control for Mobile Devices Physical Access Control Access Control for Output Devices
Authentication	Permitted Actions Without Identification/ Authentication Auditable Events Identification and Authentication Policy and Procedures Device Identification and Authentication Cryptographic Module Authentication
Encryption	Media Storage
Risk assessment	Risk Assessment Risk Assessment Policy and Procedures
Trust	Trust Path
Confidential	Personnel Screening

4.5 Summary

Overall, among the four certifications, SOC2 has the best performance on privacy protections based on the percentage of privacy-related controls. It not only includes an additional section of criteria specifically designed for privacy, but also mentions the data subjects (users) in its content and emphasizes the importance of protecting their information. Besides SOC2, C5 has a higher percentage of privacy-related controls, compared with the other two certifications. However, most of these controls from C5 only implicitly refer to privacy since C5 focuses primarily on information security. For example, the control "Encryption of sensitive data for storage" refers to the procedures and technical safeguards established by the CSP to encrypt cloud customers' data during storage. Although the control is originally designed as a security safeguard, the process of encrypting customers' data also implies privacy protections for personal information. Thus, it is counted as implicit privacy control in this case. Surprisingly, neither ISO/IEC 27011 or FedRAMP has many controls explicitly related to privacy, and both have a lower percentage of implicit privacy controls, compared with SOC2 and C5. This suggests that the concept of privacy might be combined with security when developing the controls. Thus, explicit privacy controls are rarely identified in these certifications.

In addition to the overall analysis of controls, for the implicit privacy controls in these four certifications, we recorded the field of privacy to which that the controls are related. The number of controls per certification for each field are shown in Figure 2. As shown in the figure, all four certifications mentioned “Access control” as part of their privacy protections. Besides Access control, “Authentication”, “Identification”, and “Risk assessment” are the three fields with most implicit privacy controls. The results once again imply that privacy is often combined with security controls instead of being explicitly implemented.

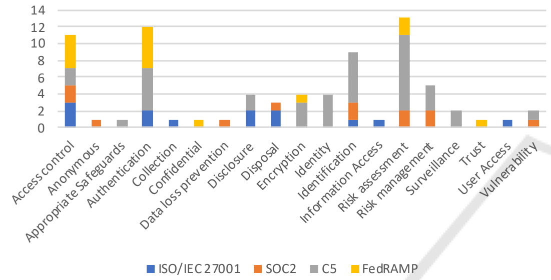

Figure 2: # of implicit privacy controls in each field.

5 DISCUSSION

Based on the results shown in the preceding section, we conclude that most of the certifications analysed in this study heavily emphasize security controls, and privacy protections are rarely mentioned. The one exception is SOC2, which includes an additional section specifically focused on privacy protections and offers actual privacy criteria so that privacy protections can be addressed. However, most privacy-related controls from other certifications are often indirect and ambiguous, in that some mention privacy only as part of the concept instead of directly discussing it. Therefore, the certifications must define their privacy controls more explicitly in the content to address the privacy considerations adequately.

Another finding is that it is sometimes difficult to distinguish between privacy and security when you examine cloud certification controls. For example, both C5 and FedRAMP include controls that provide privacy protections (i.e., controls related to encryption), even though it is not explicitly required or stated. Although the techniques of encryption are often used or required to help with protecting information security, the process of information would also help to protect users’ privacy by restricting access to their personal and sensitive information. Thus, we included such controls in our assessment and coded them as Privacy-Implicit, meaning that while the control is meant for security protections, it also provides implicit privacy protections. Also, since C5 was designed by the Federal Office for Information Security (BSI) in Germany to help organizations demonstrate operational security against common cyber-attacks, all the controls in C5 were originally developed as security controls; therefore, many of the privacy-related controls in C5 are based on information security protections, with privacy being implied in the content of the control.

A challenging aspect of our study is that, unlike cloud security, cloud privacy is a new field without widely applied or referenced existing guidelines or standards. It was difficult for us to evaluate each certification’s privacy performance because there was neither much prior literature nor established frameworks that could serve as the baseline for evaluation. Although FIPPs has been applied for a long time and been implemented in a variety of fields, it has limitations because cloud computing technologies developed so rapidly. Therefore, this study points to the need to build a comprehensive and systematic framework that includes all the essential criteria for information privacy protections in cloud computing as a standard for evaluating certifications in the future.

6 STUDY LIMITATIONS

As mentioned above, the certification versions analysed for this study were the most recent versions that are publicly available online. We realize that it would be ideal to use the most recent version of the certifications, However, some of the updated documentations are not publicly available online. Therefore, we acknowledge that our results may be influenced by this factor and hence it is possible that there exist new updated versions of the four certifications mentioned in this study that may include privacy-specified controls in the content.

Another limitation of this study is that since we did not have a widely applied guideline or standard to evaluate the certification’s performance on privacy protections, we defined a list of privacy terminologies from multiple sources to help with examining the relevancy of privacy for each control. However, it is possible that some terms are missing from the list, or that some terms may not be strongly related to privacy under certain conditions. Results from this study still need to be verified with a comprehensive standard to ensure its effectiveness and accuracy.

7 FUTURE WORK

In conclusion, this study points out the need for addressing privacy challenges in cloud environments, and builds initial step towards developing a comprehensive set of privacy controls which can be used for assessing and comparing these four certifications and their shortcomings. Results will also benefit governments and industry when comparing different certifications for their privacy protections and selecting the appropriate one based on specific needs.

For future studies, it is necessary to develop a consistent and comprehensive framework for cloud computing privacy protections in order to evaluate and verify the certification performance in a more accurate and effective way. We will continue to work on analysing the content of cloud certifications with a more inclusive selection of sources and continue updating the results based on the latest version of the certifications as they become available.

ACKNOWLEDGEMENTS

This work has been supported by Cisco Inc. We want to acknowledge and thank all of those who have contributed to this work.

REFERENCES

Leymann, F., & Fritsch, D. (2009). Cloud computing: The next revolution in IT. *Proceedings of the 52th Photogrammetric Week,* 3-12.

Perera, C., Ranjan, R., Wang, L., Khan, S., & Zomaya, A. (2015). Privacy of big data in the internet of things era. *IEEE IT Special Issue Internet of Anything*, *6*.

Gahi, Y., Guennoun, M., & Mouftah, H. T. (2016, June). Big data analytics: Security and privacy challenges. In *2016 IEEE Symposium on Computers and Communication (ISCC)* (pp. 952-957). IEEE.

Guilloteau, S., & Venkatesen, M. (2013). Privacy in Cloud Computing-ITU-T Technology Watch Report March 2012.013

Gai, K., Qiu, M., Zhao, H., & Xiong, J. (2016, June). Privacy-aware adaptive data encryption strategy of big data in cloud computing. In *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 273-278). IEEE.

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., & Bashir, M. N. (2017, March). Cloud security certifications: a comparison to improve cloud service provider security. In *Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing* (pp. 1-12).

Lar, S. U., Liao, X., & Abbas, S. A. (2011, August). Cloud computing privacy & security global issues, challenges, & mechanisms. In *2011 6th International ICST Conference on Communications and Networking in China (CHINACOM)* (pp. 1240-1245). IEEE.

Kumar, S. N., & Vajpayee, A. (2016). A survey on secure cloud: security and privacy in cloud computing. *American Journal of Systems and Software*, *4*(1), 14-26.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903.

Kang, M., & Kwon, H. Y. (2019, January). A study on the needs for enhancement of personal information protection in cloud computing security certification system. In *2019 International Conference on Platform Technology and Service (PlatCon)* (pp. 1-5). IEEE.

Anisetti, M., Ardagna, C. A., Damiani, E., El Ioini, N., & Gaudenzi, F. (2018). Modeling time, probability, and configuration constraints for continuous cloud service certification. *Computers & Security*, *72*, 234-254.

Karkouda, K., Nabli, A., & Gargouri, F. (2018, October). Privacy and availability in cloud data warehouse. In *Proceedings of the 10th International Conference on Education Technology and Computers* (pp. 388-391).

Teigeler, H., Lins, S., & Sunyaev, A. (2018, January). Drivers vs. inhibitors-what clinches continuous service certification adoption by cloud service providers?. In *Proceedings of the 51st Hawaii international conference on system sciences*.

Lansing, J., Schneider, S., & Sunyaev, A. (2013). Cloud service certifications: Measuring consumers' preferences for assurances.

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud! Privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (pp. 1-20).

Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic certification of cloud services: Trust, but verify!. *IEEE Security & Privacy*, *14*(2), 66-71.

Cate, F. H. (2006). The failure of fair information practice principles. *Consumer protection in the age of the information economy*.

Solove, D. & Citron, D. (2018). Risk and Anxiety: A Theory of Data-Breach Harms. *Texas Law Review 96(4)*, 737-786

Sharma, T., Wang, T., Di Giulio, C., & Bashir, M. (2020, October). Towards Inclusive Privacy Protections in the Cloud. In *International Conference on Applied Cryptography and Network Security* (pp. 337-359). Springer, Cham.